

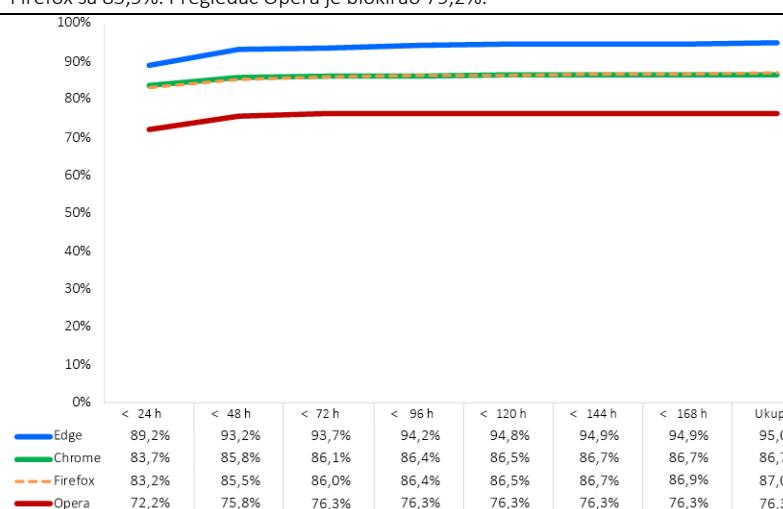
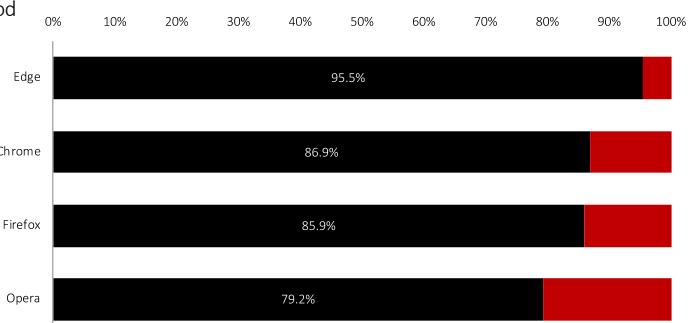
K2 2020

KOMPARATIVNI IZVEŠTAJ O TESTIRANJU

Pregled

Tokom K2 2020. kompanija NSS Labs je obavila nezavisno testiranje zaštite od phishinga koju pružaju veb pregledači: 47.274 diskretna testa (po veb pregledaču) koji koriste 2443 jedinstvene phishing URL adrese tokom 18 dana. Da bi štitio od phishinga, Microsoft Edge koristi SmartScreen filter Microsoft zaštitnika, Google Chrome i Mozilla Firefox koriste Google API za bezbedno pregledanje, a Opera koristi kombinaciju lista blokiranog sadržaja nezavisnih proizvođača.

Microsoft Edge je ponudio najbolju zaštitu, blokirao je 95,5% phishing URL adresa i istovremeno obezbedio najvišu stopu zaštite u zakazano vreme (89,2%). Google Chrome je pružio drugu po redu najbolju zaštitu, u proseku je blokirao 86,9%, a iza njega sledi Mozilla Firefox sa 85,9%. Pregledač Opera je blokirao 79,2%.

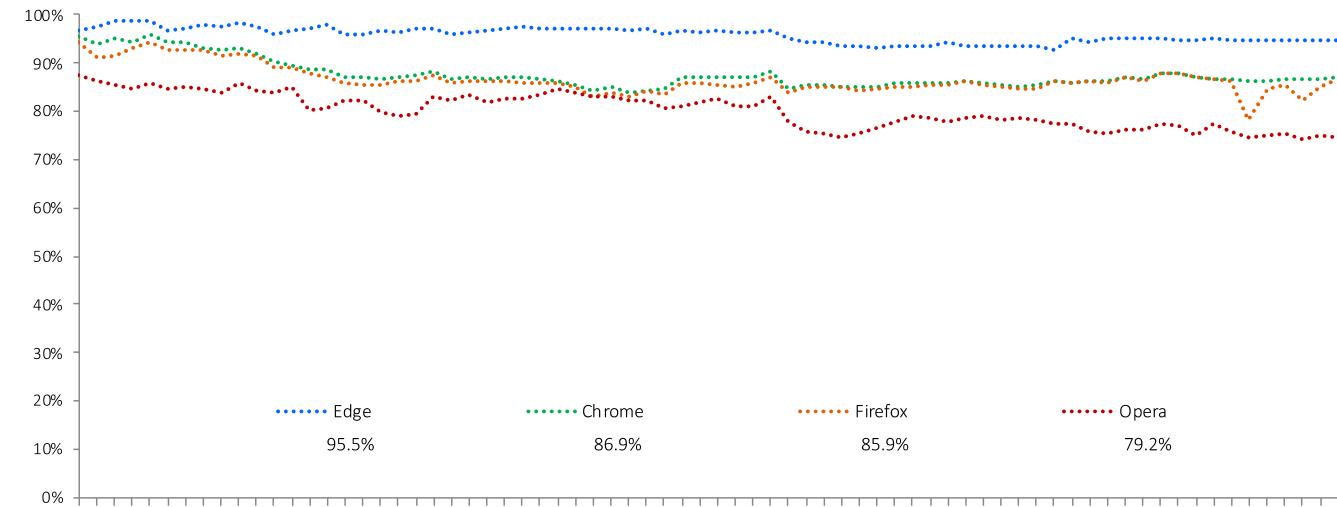


Sistemi reputacije URL adresa skraćuju vreme koje je napadačima potrebno da ostvare ciljeve tako što sprečavaju/upozoravaju korisnike da URL adresa predstavlja poznati phishing sajt. Međutim, pošto korisnici posećuju širok opseg veb sajtova, od kojih su mnogi novi, sistemi reputacije URL adresa ne mogu prosti da blokiraju sve nove URL adrese. Znajući ovo, phishing kampanje napadača se stalno menjaju, a većina svih napada se dešava u prvih nekoliko sati nakon pokretanja napada.

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

Rezime rezultata

Zaštita od phishinga tokom vremena



Tokom celokupnog testiranja, nove phishing URL adrese su se svakodnevno dodavale, a URL adrese koje više nisu bile dostupne ili više nisu isporučivale phishing napade su uklonjene. Svaka tačka podataka predstavlja zaštitu u određenom trenutku. Ako je URL adresa blokirana u početku, ocena doslednosti zaštite pregledača se poboljšala tokom vremena. U suprotnom, ako pregledač nije blokirao URL adresu, ocena se smanjila.

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

Pozadina

Phishing je tip napada društvenog inženjeringu koji pokušava da ubedi žrtvu da napadaču obezbedi osetljive lične informacije. Neki primjeri osetljivih informacija su brojevi kreditnih kartica, brojevi socijalnog osiguranja, informacije za prijavljivanje i lozinke za račune u banci. E-pošta, trenutne poruke, SMS poruke i veze na sajтовima društvenih mreža predstavljaju vektore za phishing napade. Početna stranica phishing veb sajta često takođe pokušava da tiho iskoristi računar posetioca i instalira zlonamerni softver (tzv. usputno iskorišćavanje).

Phishing napadi predstavljaju veliki rizik za pojedince i organizacije zato što prete da ugroze ili preuzmu osetljive lične i korporativne informacije. Kompanija Anti-Phishing Working Group (APWG) je prijavila ukupno 165.772 jedinstvene phishing kampanje putem e-pošte u prvom kvartalu 2020.¹ Phishing napadi postaju sve složeniji i sofisticiraniji, što otežava njihovo otkrivanje i sprečavanje.

Zaštita veb pregledača od phishinga

Zaštitu od phishinga obezbeđuje aplikacija u okviru veb pregledača koja zahteva reputaciju URL adrese od servera za reputaciju u oblaku. Server za reputaciju na internetu pretražuje phishing veb sajtove, a zatim svakoj URL adresi daje ocenu i dodaje je na listu blokiranog sadržaja. Na taj način, kada veb pregledač dobije komandu da poseti neku URL adresu, njegova zaštita od phishinga (tj. bezbedno pregledanje, SmartScreen itd.) zahteva reputaciju URL adrese od servera za reputaciju zasnovanog na tehnologiji oblaka i ako rezultati pokažu da je veb sajt „loš“, veb pregledač preusmerava korisnika na poruku upozorenja koja objašnjava da je URL adresa zlonamerna. Neki sistemi reputacije takođe uključuju dodatan obrazovni sadržaj. U suprotnom slučaju, ako se utvrdi da je veb sajt „dobar“, veb pregledač ne radi ništa i korisnik neće znati da je pregledač upravo izvršio bezbednosnu proveru.

Podaci u ovom izveštaju prikupljeni su tokom perioda testiranja od 18 dana između 21. aprila 2020. i 8. 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 phishing URL adresama, kao i uslugama reputacije pregledača u oblaku.

Naglasak je bio na svežini i zato je procenjen veći broj sajtova od onog koji je na kraju zadržan kao dobijeni skup za testiranje pošto su se nove URL adrese stalno dodavale u test, a mrtvi sajtovi su se uklanjali.

Ukupan broj zlonamernih URL adresa u testu

U svakom pregledaču je više puta testirano ukupno 4020 neobrađenih URL adresa čija valjanost nije proverena, za ukupno 222.527 diskretnih testova obavljenih bez prekida tokom 430 sati (na svakih 6 sati tokom 18 dana). NSS inženjeri su uklonili uzorke koji nisu prošli kriterijum provere valjanosti, uključujući one koji su oštećeni zloupotrebom (nisu deo ovog testa). Na kraju su 2443 jedinstvene, važeće phishing URL adrese uključene u 189.096 diskretnih, važećih testova phishinga (47.274 po veb pregledaču), što je obezbedilo marginu greške manju od 2 procenta (<2%) uz stepen pouzdanosti od 95%.

Prosečan broj dodatih zlonamernih URL adresa dnevno

U proseku se 136 novih URL adresa čija valjanost je proverena dnevno dodavalo u skup testova; brojevi su se razlikovali nekim danima kada su nivoi kriminalnih aktivnosti fluktuirali.

Blokiranje phishing URL adresa

Kompanija NSS je procenila mogućnost pregledača da blokiraju zlonamerne URL adrese čim se otkriju na internetu. Inženjeri su ponavljali ove testove na svakih šest sati da bi utvrdili koliko je vremena potrebno da proizvođač doda zaštitu, ako je uopšte i dodaje.

Novi Microsoft Edge je zasnovan na pregledaču Chromium i objavljen je 15. januara 2020. Kompatibilan je sa svim podržanim verzijama operativnih sistema Windows i macOS. Preuzimanjem ovog pregledača zameniće zastarelju verziju pregledača Microsoft Edge na Windows 10 računarama.

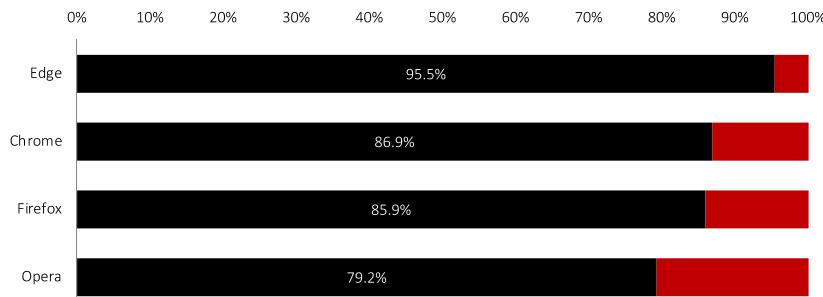
<https://support.microsoft.com/sr-rs/help/4501095/download-the-new-microsoft-edge-based-on-chromium>

¹ APWG izveštaj o trendovima phishing aktivnosti

Stopa blokiranja phishinga

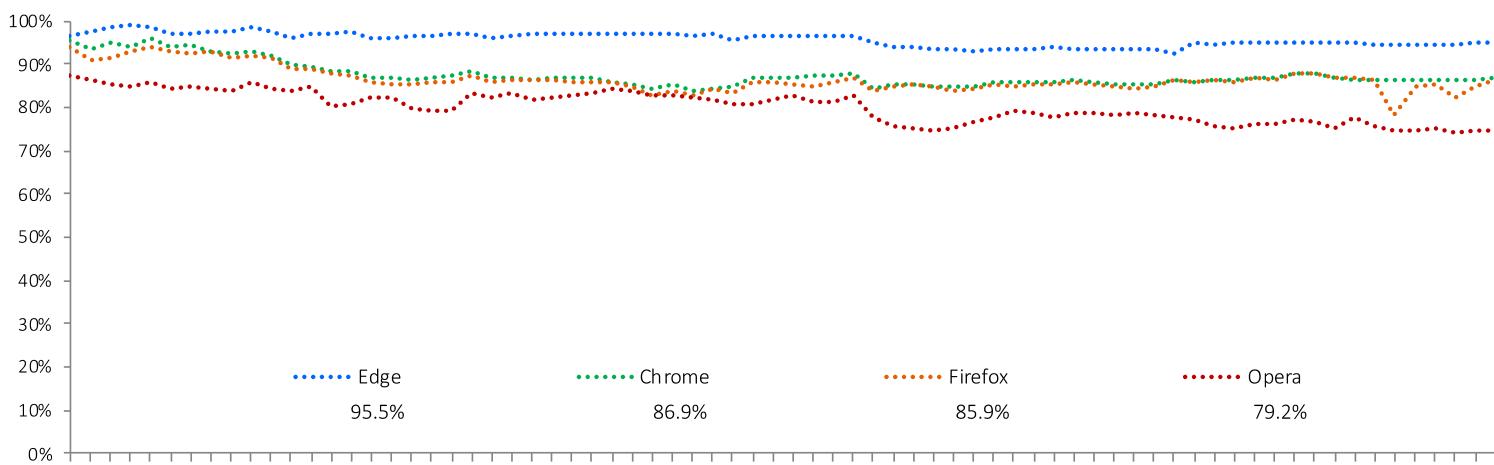
Google Chrome i Mozilla Firefox koriste Google API za bezbedno pregledanje. Microsoft Edge koristi SmartScreen filter Microsoft zaštitnika, uključujući uslugu reputacije aplikacija kako bi pružio zaštitu od phishinga i pretnji malvera. Opera koristi kombinaciju lista blokiranog sadržaja iz usluga Netcraft,² PhishTank³ i Metamask⁴, kao i listu blokiranog malvera iz usluge Yandex.⁵

Mogućnost upozoravanja potencijalnih žrtvi da će zалутати na zlonamerni veb sajt stavlja veb pregledače u jedinstven položaj za borbu protiv phishinga i drugih kriminalnih aktivnosti. Pošto phishing sajtovi 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. Ovo objašnjava korelaciju između prosečnog vremena za blokiranje i stope hvatanja. 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 phishing sajtova se blokira u prva 24 sata otkrivanja nego nakon toga.



Pojedinačne performanse blokiranja svakog pregledača merene su neprekidno i snimljena je ukupna stopa blokiranja svih URL adresa koje je testirao pregledač. Ukupna stopa blokiranja pregledača izračunava se kao broj uspešnih blokiranja podeljen ukupnim brojem slučajeva za testiranje. Na primer, u testovima koji se obavljaju na svakih 6 sati, URL adresa koja je na mreži 48 sati biće testirana 8 puta. Pregledač koji je blokira u 6 (od maksimalno 8) pokretanja testa ostvariće stopu blokiranja od 75%.

Doslednost zaštite tokom vremena



Tokom celokupnog testiranja, nove phishing URL adrese su se svakodnevno dodavale, a URL adrese koje više nisu bile dostupne ili više nisu isporučivale phishing URL adrese su uklonjene. Svaka tačka podataka predstavlja zaštitu u određenom trenutku. Ako je URL adresa blokirana u početku, ocena doslednosti zaštite pregledača se poboljšala tokom vremena. U suprotnom, ako pregledač nije blokirao URL adresu, ocena se smanjila.

² <http://www.netcraft.com/>

³ <http://www.phishtank.com/>

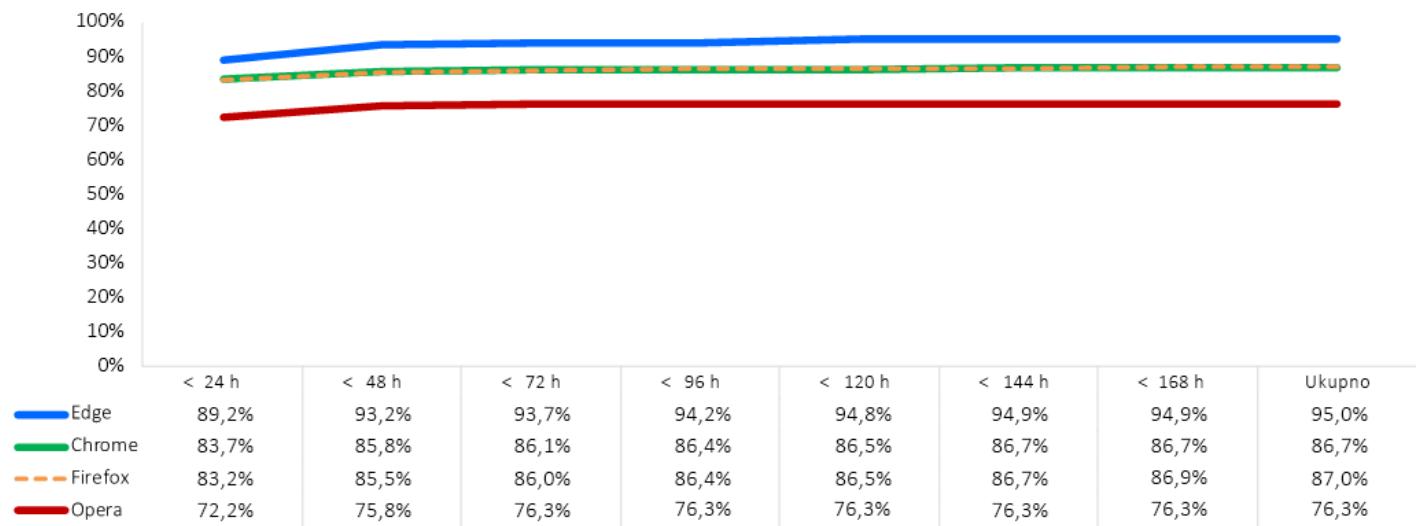
⁴ <https://github.com/metamask/eth-phishing-detect>

⁵ <https://yandex.com>

Histogram zaštite od phishinga

Trenutna zaštita od novih phishing URL adresa je od kritičnog značaja. Čim se phishing sajtovi otkriju, oni se gase, često za relativno kratko vreme. Proizvodi koji ne uspeju da dodaju zaštitu na vreme mogu zakasniti sa otklanjanjem pretnje. Dolenavedeni histogram prikazuje koliko je vremena bilo potrebno svakom pregledaču da blokira phishing sajt kada je pretnja ubaćena u ciklus testiranja. U periodu od sedam dana, kumulativne stope zaštite su se izračunavale svaki dan dok pretnje nisu bile blokirane.

Tokom testiranja, Microsoft Edge je pokazao početnu stopu zaštite od phishing napada od 89,2%. Google Chrome i Mozilla Firefox su ostvarili početnu stopu zaštite od 83,7% i 83,2%, tim redosledom. Početna stopa zaštite pregledača Opera bila je 72,2%. Do kraja sedmog dana testiranja, svi veb pregledači su postigli povećanje zaštite. Microsoft Edge je povećao zaštitu za 5,7% na 94,9%. Mozilla Firefox je povećao za 3,7% na 86,9%, Google Chrome je povećao za 3% na 86,7%. Pregledač Opera je povećao za 4,1% na 76,3%



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 – 84.0.502.0
- 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

Ovaj i drugi srodni dokumenti dostupni su na adresi: www.nsslabs.com. Da biste dobili licenciranu kopiju ili prijavili zloupotrebu, обратите se kompaniji NSS Labs.

© 2020 NSS Labs, Inc. Sva prava zadržana. Nijedan deo ove publikacije ne može da se reproducuje, kopira/skenira, uskladišti na sistemu za preuzimanje, pošalje e-poštom ili na drugi način distribuira ili prenosi bez izričitog pisanog odobrenja kompanije NSS Labs, Inc. („nas“ ili „mi“).

Pročitajte odricanje odgovornosti u ovom pakovanju zato što ono sadrži važne informacije koje vas obavezuju. Ako ne pristajete na ove uslove, ne treba da čitate ostatak ovog izveštaja, već treba odmah da nam ga vratite. „Vi“ ili „vaš/a“ predstavlja osobu koja pristupa ovom izveštaju i svaki entitet u čije ime je ta osoba nabavila izveštaj.

1. Informacije u ovom izveštaju podležu promenama bez obaveštenja i odričemo se svake obaveze da ih ažuriramo.
2. Smatramo da su informacije u ovom izveštaju precizne i pouzdane u trenutku objavljivanja, ali ne garantujemo to. Vi snosite rizik od korišćenja ovog izveštaja i oslanjanja na njega. Mi nismo odgovorni ni za kakve štete, gubitke ili troškove bilo koje prirode koji potiču od neke greške ili nečeg što je izostavljeno u ovom izveštaju.
3. MI NE DAJEMO NIKAKVE GARANCIJE, IZRIČITE ILI PODRAZUMEVANE. OVIM PUTEM SE ODRIČEMO ODGOVORNOSTI I IZUZIMAMO SVE PODRAZUMEVANE GARANCIJE, UKLJUČUJUĆI PODRAZUMEVANE GARANCIJE PODESNOSTI ZA PRODAJU, PODESNOSTI ZA ODREĐENU NAMENU I NEKRŠENJA PRAVA INTELEKTUALNE SVOJINE. NI U KOM SLUČAJU MI NEĆEMO BITI ODGOVORNI ZA DIREKTNU, NEMATERIJALNU, NENAMERNU, EGZEMPLARNU ILI INDIREKTNU ŠTETU NITI ZA GUBITAK PROFITA, PRIHODA, PODATAKA, RAČUNARSKIH PROGRAMA ILI DRUGIH RESURSA, ČAK I AKO POSTOJI OBAVEŠTENJE O TOJ MOGUĆNOSTI U NASTAVKU.
4. Ovaj izveštaj ne predstavlja podršku, preporuku niti garanciju za bilo koji testirani proizvod (hardverski ili softverski) niti za hardver i/ili softver koji su korišćeni tokom testiranja proizvoda. Testiranje ne garantuje da neće biti grešaka ili oštećenja u proizvodima niti da će proizvodi ispuniti vaša očekivanja, zahteve, potrebe ili specifikacije, kao ni da će raditi bez prekida.
5. Ovaj izveštaj ne implicira nikakvu preporuku, sponsorstvo, pripadnost ili verifikaciju od strane organizacija pomenutih u njemu.
6. Svi žigovi, oznake usluga i poslovna imena korišćeni u ovom izveštaju predstavljaju žigove, oznake usluga i poslovna imena odgovarajućih vlasnika.