CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Google Chrome sa stajališta sigurnosti

CCERT-PUBDOC-2008-10-243

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Web preglednik (eng. *browser*) je program koji korisniku omogućuje pregledavanje i interakciju sa sadržajem (tekstom, slikama, video zapisima, igrama i drugim sadržajem) koji se nalazi na web adresi. Korisniku je omogućen brz i jednostavan pristup informacijama koje su postavljene na web adresama. Web preglednici zapravo imaju funkciju prevoditelja koda kojim su napisane web stranice. Najčešće upotrebljavani kod je HTML (eng. *HyperText Markup Language*) kod. Dakle, web preglednik učitava HTML kod tražene web stranice i oblikuje ga za grafički prikaz korisniku. Postoji velik broj različitih preglednika (Internet Explorer, Mozilla Firefox, Opera, Safari, Google Chrome, itd.), a svaki od njih tumači zadani HTML kod na svoj način, tako da se ista web stranica može prikazati na drugi način u dva različita preglednika.

Web preglednici, kao i ostali programi, nisu imuni na zlonamjerne programske kodove, tako da je potrebno posvetiti pažnju sigurnosti pri pregledavanju sadržaja na Internetu. Broj napada u kojima je iskorišten neki od sigurnosnih propusta (eng. *exploit*) web preglednika u stalnom je porastu. Iako se proizvođači preglednika trude na vrijeme ispraviti propuste, mnogo korisnika osjeti posljedice sigurnosnih propusta (krađa podataka, krađa identiteta, itd.). Porastu broja napada također pridonosi nepažnja korisnika pri korištenju preglednika i posjećivanje zlonamjernih web odredišta. Ukoliko se u kod web stranice ubaci zlonamjerna skripta, postoji mogućnost da ju web preglednik učita i izvrši, čime se ugrožava sigurnost podataka na računalu. Korisnici često nisu svjesni opasnosti i posljedica neopreznog korištenja web alata.

Iz *open-source* projekta „Chromium“, kojem je cilj stvoriti sigurniji, brži i jednostavniji alat za korištenje Interneta, nastao je „Google Chrome“ - preglednik kojeg krase karakteristike poput minimalističkog izgleda, raznolike funkcionalnosti te velike brzine i jednostavnosti. „Chrome“ je trenutačno moguće preuzeti u *beta* inačici što znači da je program još uvijek u razvoju. „Google“ se odlučio na objavu *beta* inačice upravo kako bi korisnici svojim prijedlozima i pronalaženjem sigurnosnih propusta usavršili „Chrome“.

Ovaj dokument se bavi sigurnošću alata „Google Chrome“, uspoređujući ga s danas najpopularnijim web preglednicima: „Internet Explorer“ i „Mozilla Firefox“.

2. Sigurnost web preglednika

Gotovo svi web preglednici imaju sigurnosne propuste što omogućava napadačima da se okoriste na štetu korisnika. Bez obzira na sigurnosne propuste, pretraživanje Interneta nije toliko rizično koliko se čini. Napadač nije u mogućnosti odabrati vrijeme i mjesto napada, već mora čekati da žrtva posjeti njegovu zlonamjernu web stranicu. U tom slučaju napadač može onemogućiti korisniku pristup vlastitom računalu, ukrasti mu datoteke (i informacije), pa čak i dobiti ovlasti na žrtvinom računalu da briše datoteke, ubacuje zlonamjerne programe ili ostavlja programe za nadgledanje korisnikove aktivnosti.

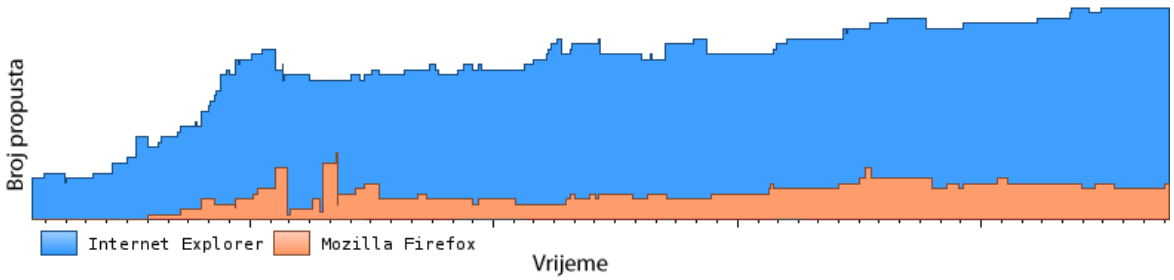
2.1. Statistike

Prema izvješćima tvrtke Secunia, stručnjaka za područje računalne sigurnosti i otkrivanje sigurnosnih propusta, u gotovo svim web preglednicima za operativni sustav Windows su nađeni sigurnosni propusti razvrstani u tri kategorije:

- srednje opasni,
- kritični i
- vrlo kritični.

Statistički podaci o sigurnosnim propustima su obrađeni za dva najpopularnija web preglednika na tržištu:

- Internet Explorer
- Mozilla Firefox



Slika 1. Broj sigurnosnih propusta u pojedinom pregledniku - Secunia

2.1.1. Internet Explorer

Internet Explorer je najčešće korišteni preglednik zbog činjenice da su sve verzije programa do Internet Explorera 6 bile ugrađene uz operativni sustav Windows. Novije inačice preglednika je moguće preuzeti izravno sa stranica Microsofta. Prema službenim statistikama tvrtke Net Applications, Microsoftov preglednik Internet Explorer drži najveći udio na tržištu, čak 71.52%, no treba uzeti u obzir da se informacije o udjelu stalno mijenjaju.

Iako ga većina korisnika upotrebljava za pregledavanje sadržaja na Internetu, podaci tvrtke Secunia ne govore u prilog Internet Exploreru kao pouzdanom i sigurnom pregledniku. Pri statističkoj obradi podataka u obzir je uzet cjelokupni dosadašnji životni vijek proizvoda, a ne najnovije verzije.

U životnom vijeku Internet Explorera prijavljena su 137 sigurnosna propusta, od kojih je:

- 25 srednje opasnih
- 48 kritičnih i
- 15 vrlo kritičnih.

Od ukupnog broja od 137 propusta preostalo je 39 koji nisu ispravljeni i to: 10 srednje opasnih i jedan vrlo kritičan propust. Velik broj propusta u Internet Exploreru je otkrio i ispravio proizvođač prije nego što su dospjeli u javnost. Ovaj preglednik prednjači po broju propusta, pogotovo kada je u pitanju broj propusta koje su napadači otkrili, a proizvođač nije ispravio. Korisnike je ugrožavalo 96 propusta u programu koji su postali dostupni u javnosti, od kojih je 11 propusta označeno vrlo kritičnima. Također se smatra važnim i vrijeme koje je potrebno proizvođaču da bi ispravio

sigurnosni propust koji je izašao u javnost. Za Internet Explorer to je u prosjeku 9 dana od otkrivanja propusta.

2.1.2. Mozilla Firefox

Mozilla Firefox je besplatni preglednik kojeg je moguće preuzeti s web stranica tvrtke Mozilla. Trenutno zauzima drugo mjesto po udjelu na tržištu od čak 19.46%. Ova pozitivna statistika rezultat je jednostavnosti, prilagodljivosti i funkcionalnosti koju Firefox posjeduje.

Tijekom životnog vijeka Mozilla Firefox-a prijavljena su 73 sigurnosna propusta, od kojih je:

- 19 srednje opasnih i
- 28 kritičnih.

Od ukupnog broja od 73 propusta preostalo je 6 „nezakrpanih" propusta, pri čemu je jedan označen kao kritičan. Važan podatak je da je Mozilli potreban u prosjeku samo jedan dan kako bi ispravio sigurnosni propust koji je dostupan u javnosti. Brza reakcija je ključna stvar pri zaštiti korisnika od zlonamjernih napada, što Firefoxu daje veliku prednost nad Internet Explorerom.

2.2. Vrste propusta

Napadač može na mnogo načina ugroziti sigurnost računala korisnika kada su u pitanju napadi putem web preglednika. Među najčešćima je napad na JavaScript programski kod kojeg upotrebljava većina web preglednika. JavaScript programski kod se koristi pri interakciji klijenta i poslužitelja. Napadač ovaj propust može iskoristiti čak i ako korisnik ima aktiviran vatrozid (eng. *firewall*). Web preglednici preuzimaju i pokreću JavaScript kod koji se nalazi unutar stranice koju je korisnik posjetio. Ovaj sigurnosni propust dozvoljava napadačima da nadgledaju korisnikovu aktivnost pri korištenju web preglednika na način da:

- promatraju web adrese dokumenata koji su učitani putem preglednika,
- promatraju korisničke podatke koje korisnici upisuju pri prijavi na neki Internet servis ili
- promatraju kolačiće (eng. cookies) pohranjene na računalu korisnika.

Napadač u JavaScript programski kod može ubaciti zlonamjerni kod poput virusa, *keyloggera* (zlonamjerni program koji pamti što je korisnik utipkao i šalje napadaču), crva, trojanca ili čak *rootkita* (zlonamjerni program koji omogućava napadaču izravno spajanje na korisničko računalo i preuzimanja kontrole nad računalom).

Uslijed povećanja broja proizvođača koji uz svoje proizvode daju ActiveX kontrole u zadnje dvije godine napadi zbog sigurnosnih propusta u ActiveX kontrolama su u porastu. Napadač iskorištavanjem ovih sigurnosnih propusta može otkriti povjerljive i osobne podatke ili u najgorem slučaju pokrenuti proizvoljni zlonamjerni programski kod na računalu žrtve. Proizvođači programskih paketa se koriste ActiveX kontrolama kako bi izvršili određenu funkciju ili niz funkcija (npr. instalacija putem Interneta). Glavna namjena ActiveX kontrola jest omogućavanje funkcionalnosti (instalacija, bolji grafički prikaz, mogućnosti u izbornicima) programima koji se nalaze na Internetu, a učitavaju se unutar web preglednika. To mogu biti programi za prikupljanje podataka, učitavanje određenih vrsta datoteka ili prikaz animiranih slika. Radi osiguranja, u web preglednike je ugrađen alat koji pri pokretanju ActiveX kontrole provjerava sadrži li ona zlonamjerni programski kod. Ukoliko preglednik prepozna da se radi o zlonamjernom kodu unutar ActiveX kontrole, odbija ju izvršiti.

U većinu novih preglednika su ugrađeni *phishing* filtri koji sprječavaju napade s namjerom krađe identiteta. Napadač može krivotvoriti web stranice raznih organizacija, poput društvenih portala, web stranica banaka, itd., kako bi se domogao povjerljivih i osobnih korisničkih podataka. Napadač se također može poslužiti krivotvorenom adresnom trakom u pregledniku tako da se korisniku čini da je posjetio stranicu koju je želio. No, kako je prije navedeno, novi preglednici imaju ugrađene filtre koji prema listi prijavljenih *phishing* web stranica upozoravaju korisnika da se radi o krivotvorini. Proizvođači preglednika takve liste redovito nadograđuju kako bi korisnicima svojih proizvoda omogućili nesmetano pretraživanje Interneta i sigurnost od krađe povjerljivih i osobnih podataka.

3. Sigurnosni elementi web preglednika

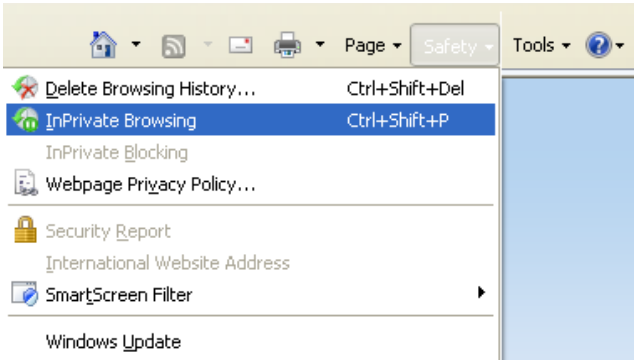
Internet Explorer i Mozilla Firefox su dva najčešće korištena preglednika, stoga je vrlo važno da na primjeren način štite korisnike od gubitka ili krađe podataka. U nastavku će biti dan pregled zaštitnih metoda koje koriste ova dva preglednika.

3.1. Internet Explorer

Usprkos činjenici da Internet Explorer ima najviše sigurnosnih propusta tijekom životnog vijeka među komercijalnim preglednicima, Microsoft stalno pokušava zaštititi korisnike alatima koje ugrađuje u sam Internet Explorer. Najnovija verzija, Internet Explorer 8, je još uvijek testna, „beta" verzija na kojoj se stalno radi.

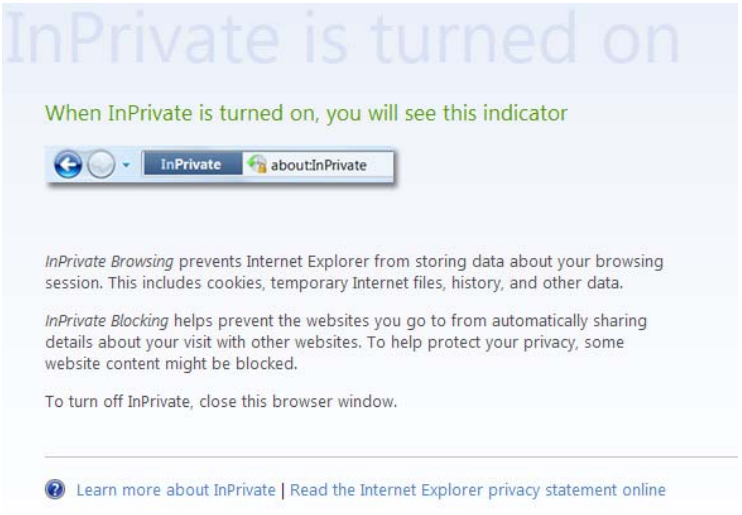
3.1.1. InPrivate način rada

Jedan od modula koje je Microsoft ugradio u Internet Explorer 8 je komponenta „InPrivate". Funkcija ove komponente je da ne dozvoljava Internet Exploreru da pamti razmjenu podataka tijekom pregledavanja web sadržaja. Ovaj alat je koristan jer uklanja tragove o posjećenim web stranicama, što se može pokazati korisnim ako više korisnika koristi isto računalo ili u slučaju da napadač želi pregledati stranice koje korisnik najčešće posjećuje. InPrivate način rada se pokreće u izborniku Sigurnost (eng. *Safety*) koji se nalazi s lijeve strane u Internet Exploreru.



Slika 2. Uključivanje InPrivate načina rada

Kada korisnik pokrene InPrivate način pregledavanja, Internet Explorer se otvori u novom prozoru. InPrivate zaštita djeluje jedino dok korisnik upotrebljava taj prozor bez obzira koliko je kartica (eng. *tab*) u prozoru otvoreno. Pokretanjem InPrivate načina rada Internet Explorer korisniku prikazuje da je pokrenut traženi način rada.



Slika 3. Aktivacija InPrivate načina rada

InPrivate zaštita zapravo tijekom pregledavanja sadržaja Internet-a pohranjuje podatke o posjećenim stranicama, ali ih nakon zatvaranja prozora u kojem je pokrenut InPrivate automatski briše.

U nastavku su navedeni podaci koji se pohranjuju tijekom pregledavanja Internet sadržaja i koje InPrivate zaštita odbacuje nakon zatvaranja preglednika:

- Kolačići - čuvaju se u memoriji tijekom pregledavanja, ali se brišu nakon zatvaranja preglednika
- Privremene Internet datoteke (eng. *Temporary Internet files*) - pohranjuju se na tvrdom disku računala, ali se brišu nakon zatvaranja preglednika
- Povijest posjećenih web stranica (eng. *Webpage history*) - podaci se ne pohranjuju
- Korisnička imena i lozinke - podaci se ne pohranjuju
- Anti-phishing priručna memorija (eng. *Anti-phishing cache*) - podaci se privremeno pohranjuju i zaštićuju kako bi web stranice bile ispravno prikazane
- Podaci iz adresne trake i AutoComplete funkcije - podaci se ne pohranjuju
- Podaci za automatsko ponovno pokretanje preglednika uslijed „rušenja“ (eng. *Automatic Crash Recovery*) - ukoliko se prozor u kojem je aktiviran InPrivate „sruši“ svi podaci se brišu
- Sustav za pohranu podataka unutar web aplikacije (eng. *Document Object Model storage*) - ovaj se sustav može zloupotrijebiti kako bi druga osoba zadržala podatke koje je korisnik upisao u neki web formular, tako da se automatski brišu nakon zatvaranja prozora preglednika

Nabrojane su mjere sigurnosti koje InPrivate koristi kako bi zaštitio korisnika, ali InPrivate nije u mogućnosti napraviti slijedeće:

- Nije moguće sakriti podatke o posjećenim stranicama od druge osobe na mrežnom sustavu, poput administratora ili zlonamjernog napadača koji je narušio sigurnost mrežnog sustava.
- InPrivate način rada ne omogućuje korisniku potpunu anonimnost pri korištenju Interneta. To znači da posjećene stranice mogu prepoznati korisnika po njegovoj web adresi ili zapisati podatke koje je korisnik unio u stranicu.
- InPrivate način rada ne briše podatke ili povijest pregledavanja koji su pohranjeni na računalu korisnika pomoću dodataka (eng. *add-ons*) u pregledniku.
- Sve stranice koje korisnik doda u omiljene web stranice (eng. *Favorites*) i vijesti koje želi primati od nekog izvora (eng. *feed*) ostati će pohranjene.

3.1.2. InPrivate blokiranje

Web stranice koje korisnici posjećuju uzimaju sadržaj (slike, oglase, itd.) iz više izvora, tj. s web stranica treće osobe. Web stranice treće osobe mogu prikupljati podatke o korisniku (stranice koje posjećuje, sadržaj koji je preuzeo, statistike, itd.), stoga InPrivate blokira sadržaj koji se preuzima s web stranice treće osobe. InPrivate blokiranje omogućava novu dimenziju zaštite korisnika tako što ograničava podatke koje neka web stranica može prikupiti i to ovisno o željenoj razini zaštite korisnika.

3.1.3. SmartScreen filtar

Današnje web stranice postaju sve složenije zbog sadržaja i funkcionalnosti u njima. Isto tako se povećava broj načina na koji napadači mogu oštetiti računalo korisnika. SmartScreen filtar je nastao iz iskustava prikupljenih iz područja zaštite od phishinga, a dodane su nove funkcije poput zaštite od instalacije zlonamjernih programa koji mogu ugroziti korisnikove datoteke, osobne podatke ili napraviti štetu. SmartScreen filtar štiti korisnika na tri načina:

- Dok korisnik pregledava Internet sadržaje SmartScreen radi u pozadini analizirajući sadržaje web stranice kako bi otkrio radi li se o zlonamjernoj ili krivotvorenoj stranici. Ako

mu se stranica učini sumnjivom, prikazat će korisniku dijaloški okvir u kojem će ga upozoriti na oprez.

- SmartScreen filtar uspoređuje stranice koje korisnik posjećuje s popisom phishing stranica i prikazuje korisniku okvir dijaloga crvene boje u kojem piše da se radi o phishing stranici. Korisniku nudi mogućnost da se vrati na početnu stranicu (eng. *Homepage*) ili da nastavi na upisanu stranicu.

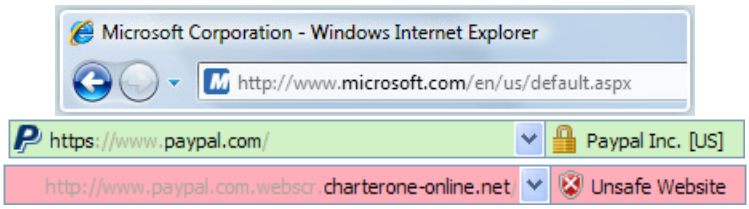
Slika 4. Prikaz upozorenja za phishing stranicu

- SmartScreen filtar također pregledava datoteke koje se preuzimaju s Interneta, te uspoređuje stranice s kojih su datoteke preuzete sa listom phishing web stranica. Ukoliko otkrije da je neka od datoteka preuzeta s jedne od prijavljenih phishing web stranica, ta datoteka biva blokirana i proces preuzimanja se zaustavlja. Popis phishing web stranica se automatski preuzima sa Microsoftovih stranica i svakodnevno se nadograđuje.

U SmartScreen filtar su uključeni još i *Cross-site scripting (XSS)* filtar, alat za isticanje domene te alat za sprječavanje pokretanja zlonamjernog programskog koda (eng. *Data Execution Prevention*).

Cross-site scripting (XSS) napadi koji prisiljavaju web aplikaciju da korisniku proslijedi zlonamjerni izvršni kod, koji se zatim učitava i izvršava u korisnikovom web pregledniku su spriječeni ovim alatom.

Alat za isticanje domene djeluje tako da domenu web stranice označi crnim slovima, a ostatak sadržaja adrese sivim.



Slika 5. Prikaz djelovanja alata za isticanje domene

Alat za sprječavanje pokretanja zlonamjernog programskog koda je sigurnosna postavka koja može spriječiti količinu štete koju virusi, crvi, trojanci i ostali zlonamjerni programi mogu načiniti na računalu korisnika na način da spriječi dio koda da se upiše u radnu memoriju.

3.2. Sigurnosni propusti u Internet Explorer 8 beta

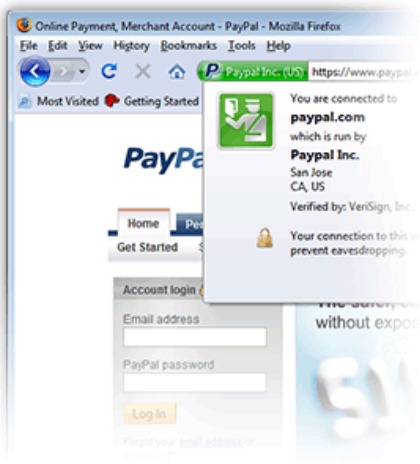
Microsoft se u posljednje vrijeme pokazuje kao proizvođač koji želi svojim korisnicima omogućiti maksimalnu sigurnost pri pregledavanju sadržaja Interneta pomoću Internet Explorera 8 beta. Zasada je nađeno nekoliko sigurnosnih propusta vezanih uz ActiveX kontrole i prikaz HTML koda. Svi propusti su označeni kao kritični i zakrpe su ubrzo objavljene. Ti su propusti omogućavali napadaču izvršavanje zlonamjernog programskog koda na računalu korisnika i stjecanje razine ovlasti korisnika, što bi značilo da je napadač mogao brisati, uništiti, ukrasti ili oštetiti datoteke i podatke korisnika.

Svi dosad pronađeni propusti za preglednik Internet Explorer 8 beta su ispravljeni.

3.3. Pregled sigurnosti Mozilla Firefox preglednika

Iako Mozilla Firefox glasi kao jedan od najsigurnijih preglednika, u protekloj - 2007. godini u njemu je pronađeno najviše sigurnosnih propusta, čak njih 88. U Mozilla Firefox inačice 3 poboljšani su sigurnosni alati iz prethodnih inačica i uvedeni neki novi.

- Brza provjera identiteta web stranice je ugrađena kako bi se zaštitilo korisnika od krivotvorenih stranica i krađe identiteta pri upisivanju podataka. Ova provjera omogućava korisniku da bude siguran pri Internet kupovini, upisivanju korisničkih imena i lozinki, itd. Omogućen je prikaz identiteta stranice s podacima o imenu tvrtke, njezine adrese i države gdje se nalazi. Također jer omogućen prikaz statistika kao što su broj posjeta stranici i da li su lozinka i korisničko ime zabilježeni na stranici.

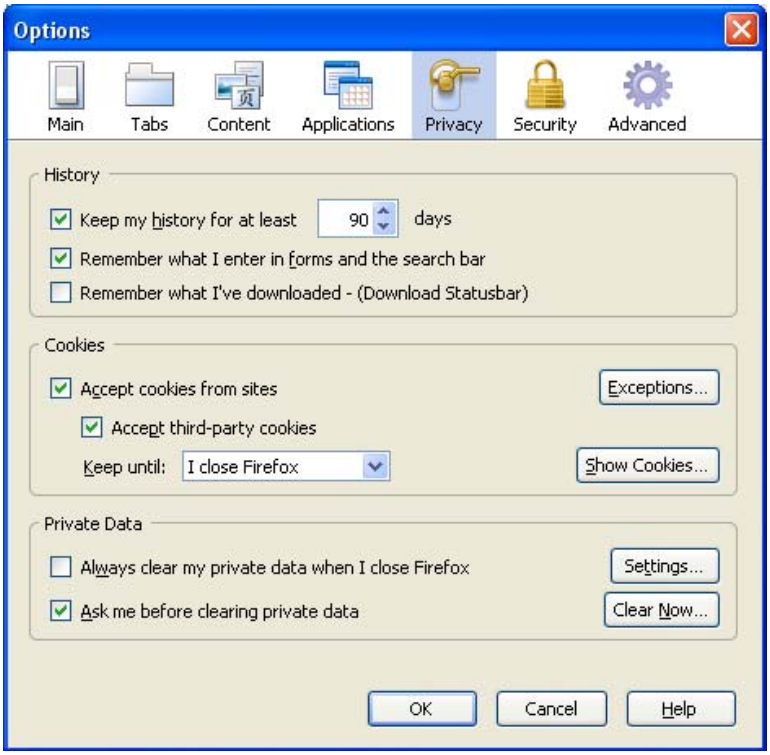


Slika 6. Prikaz brze provjere identiteta web stranica

- Alat za otkrivanje zlonamjernih programa (eng. *Anti-Malware*) štiti korisnike od virusa, crva, trojanaca i drugih zlonamjernih programa. Ako korisnik nesvjesno učita zlonamjernu web stranicu, Firefox će odmah prikazati dijaloški okvir koji će upozoriti korisnika da se radi o stranici koja sadržava zlonamjerni programski kod. Mozilla svakodnevno nadograđuje popis zlonamjernih stranica i Firefox automatski preuzima taj popis.
- Anti-Phishing alat omogućuje da Mozilla Firefox otkrije krivotvorene stranice i zaštiti korisnika od krađe identiteta i nanošenja financijske štete. Kada preglednik pokuša učitati stranicu koja je prijavljena kao phishing web stranica, korisnik dobiva upozorenje da se radi o takvoj stranici.

Slika 7. Prikaz okvira dijaloga pri otkrivanju phishing web stranice

- Pri korištenju Mozilla Firefox preglednika u kombinaciji s operativnim sustavom Windows, omogućena je integracija antivirusnog alata s preglednikom. Nakon preuzimanja datoteke s Interneta, antivirusni alat je pregledava kako se računalo korisnika ne bi zarazilo nekim od zlonamjernih programa poput virusa, crva ili trojanca.
- Čišćenje osobnih podataka poput posjećenih stranica, kolačića ili spremljenih korisničkih imena i lozinki moguće je napraviti samo jednim klikom miša. Korisnicima je omogućen odabir razine sigurnosti. U izborniku Alati>Postavke u kartici Privatnost prikazane su mogućnosti zaštite. Korisnik svojim odabirom može odlučiti koliko dugo vremenski želi čuvati povijest posjećenih stranica, povijest datoteka koje je preuzeo ili podatke koje je unosio u formulare na Internetu, te čuvanje kolačića.



Slika 8. Prikaz mogućnosti izbornika Privatnost

- Roditeljska zaštita u programu omogućuje postavljanje lozinke za pristup pregledniku. Na ovaj način se sprječava da djeca pregledavaju sadržaje koji nisu prilagođeni njihovoj dobi i/ili sprječava napadača da prevari djecu radi dobivanja povjerljivih i osobnih korisničkih podataka. Ova funkcija omogućena je na operativnom sustavu Windows Vista.
- Automatska aktualizacija programa pruža korisniku višu razinu sigurnosti. Ako se pojavi nadogradnja za Firefox preglednik, korisniku se prikazuje obavijest da je moguće preuzeti

najnoviju verziju. Korisniku je u mogućnosti odabrati na koji način želi da se nadogradnja odvija, automatski ili da se, svaki puta kada se pojavi nova verzija programa, pokaže dijaloški okvir u kojem korisnik odabire što želi učiniti.

3.4. Sigurnosni propusti u Mozilli Firefox 3

Propust označen kao MFSA 2008-34 u proizvođačevoj bazi podataka, dopuštao je napadaču izvršavanje proizvoljnog programskog koda na računalu korisnika, a uzrokovano je pretrpavanjem CSS (eng. *Cascading Style Sheets*) brojača za usmjeravanje. Kada bi se brojač pretrpao prevelikom količinom podataka, obično bi se dogodilo da se preglednik „sruši". Kada se preglednik „sruši" napadač može pokrenuti izvršavanje proizvoljnog programskog koda na računalu korisnika. Ovaj propust označen je kao kritičan i ispravljen nekoliko sati nakon otkrivanja.

Propust vezan uz pokretanje Mozille putem nekog drugog Internet alata označen je kritičnim. Napadaču nije davao nikakvu razinu ovlasti na računalu žrtve. Kao najgori slučaj iskorištavanja ovog propusta navedeno je zavaravanje (eng. *spoofing*), gdje napadač na prijevaru od korisnika pokušava doznati povjerljive i osobne podatke krivotvoreći svoj stvarni identitet. Ovaj propust je ispravljen.

Također, uočen je i prijavljen propust vezan uz napad putem grafičke GIF (eng. *Graphics Interchange Format*) datoteke koja se učita u Firefox preglednik. Ovaj propust vezan je uz Mac OS X operativne sustave. Omogućava napadaču nasilno gašenje preglednika i pokretanje proizvoljnog programskog koda na računalu korisnika. Ovaj je propust označen je kao kritičan i vrlo ubrzo ispravljen.

U 3.0.2 inačici Mozilla Firefox preglednika pronađeno je još 5 sigurnosnih propusta, od kojih su 2 označena kao kritična, 2 kao srednje opasna i jedan niskog stupnja rizika. Za jedan od nađenih propusta kao najgora posljedica navedeno je izvršavanje proizvoljnog programskog koda, dok ostali nisu ugrožavali računalo korisnika.

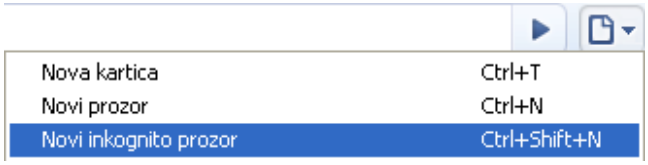
4. Sigurnosni elementi Google Chrome *beta* web preglednika

Google se odlučio uključiti u rat preglednika svojim preglednikom otvorenog koda - Google Chrome-om. Google Chrome preglednik je besplatan, a moguće ga je preuzeti sa službenih stranica Google-a. Jednostavnost i funkcionalnost su zaintrigirali većinu korisnika, no sigurnost pri pregledavanju Interneta bi trebala biti na prvom mjestu. Google Chrome je zasada isprobao velik broj korisnika, a prema izvješću tvrtke Net Applications udio Google Chrome na tržištu iznosi 0.78%.U nastavku se nalazi pregled modula koje Chrome koristi u zaštiti korisnika na Internetu.

4.1. Inkognito način rada

Slično kao i kod Internet Explorera 8 beta, u pregledniku Google Chrome je moguće raditi u potpunoj privatnosti. Inkognito način rada omogućuje korisniku maksimalnu razinu privatnosti pri pregledavanju sadržaja na Internetu. Bilo da se radi o računalu koje koristi više osoba ili radi prevencije zbog napada, Inkognito način rada ne pamti informacije koje je korisnik unio u preglednik upisujući korisnička imena i lozinke, ispunjavajući formulare ili povijest pregledanih stranica.

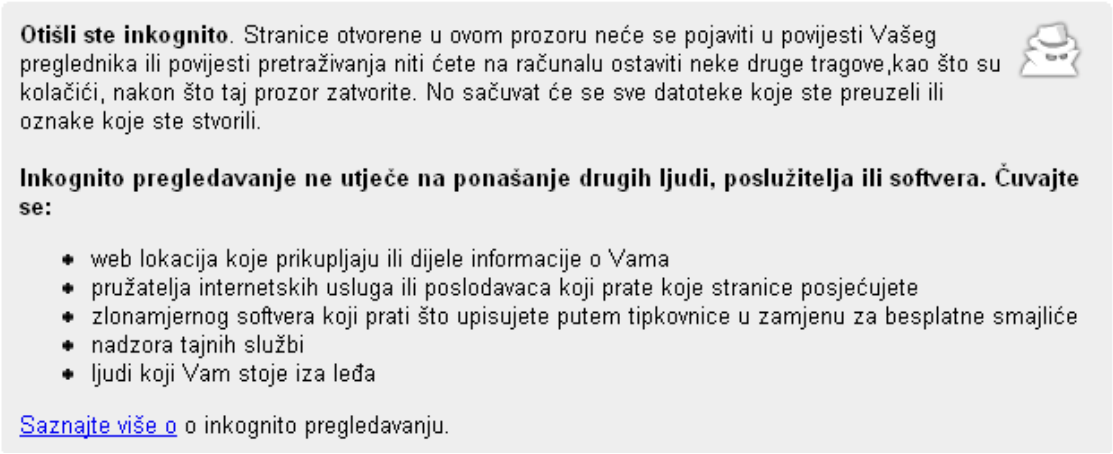
Prozor u kojem je aktiviran Inkognito se otvara zasebno od prethodno otvorenog prozora, tako da je moguće raditi i u normalnom načinu i u anonimnom (Inkognito). Ovaj način rada moguće je pokrenuti u izborniku „Stranica“ odabirom „Novi inkognito prozor“.



Slika 9. Prikaz uključivanja Inkognito načina rada

Inkognito način rada se također može aktivirati pritiskom na desnu tipku miša i odabirom „Otvaranje veze u inkognito prozoru“.

Kada je aktiviran Inkognito, u gornjem lijevom kutu preglednika će se pojaviti ikona koja to označava. Nakon aktivacije, u izborniku se pojavi kratko objašnjenje Inkognito načina rada gdje su navedena također i neka upozorenja korisnicima.



Slika 10. Objašnjenje unutar Inkognito prozora

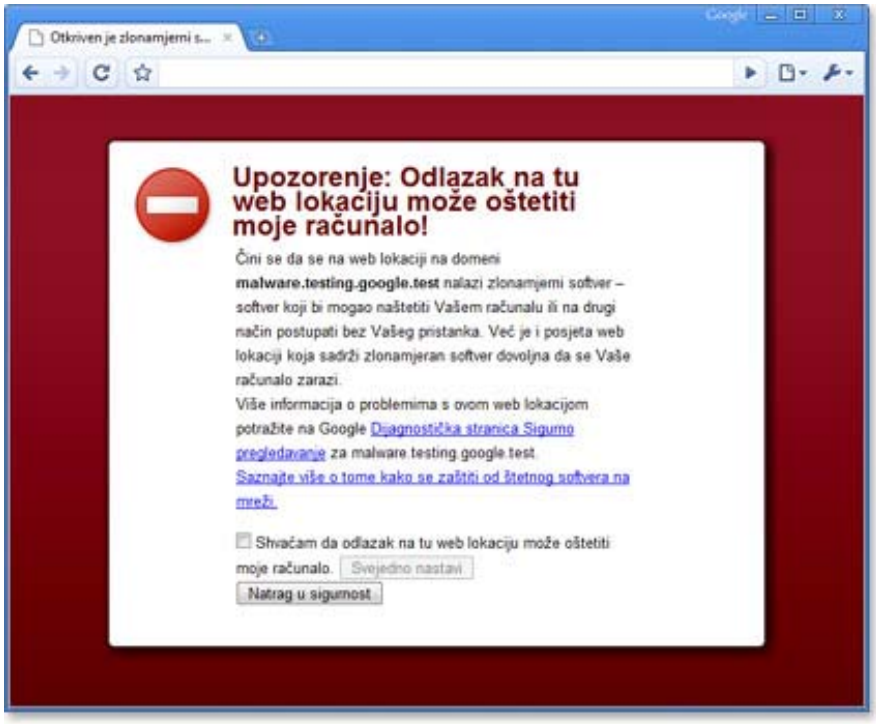
Zaštita je svakako učinkovita jer ne postoje gotovo nikakvi tragovi na računalu koji bi mogli na bilo koji način ugroziti korisnika, ako je pokušaj napada u pitanju. Podaci poput kolačića koji su preuzeti tijekom pregledavanja u Inkognito načinu rada se automatski brišu nakon zatvaranja prozora. Međutim, činjenica je da stranice koje korisnik posjeti mogu zapisivati statistike o posjetima. Također je moguće da, ukoliko se računalo nalazi u nekom mrežnom sustavu, administrator tog sustava može imati uvid u evidenciju

posjećenih stranica, čak i ako je korisnik pregledavao Internet sadržaj u Inkognito načinu rada. Tako da se Inkognito zapravo odnosi na lokalnu anonimnost na računalu koje je korisnik upotrijebio.

4.2. Phishing i spoofing zaštita

Pošto su napadi na računala sve češći, u Google Chrome je ugrađena zaštita koja donekle štiti korisnika od zlonamjernih programa i otuđivanja osobnih podataka. Moduli za obranu od spoofing i phishing napada su objedinjeni u jedan alat koji korisnika upozorava na zlonamjerne ili krivotvorene stranice.

Način rada ovog alata je sljedeći: ako korisnik utipka krivotvorenu ili zlonamjernu adresu u adresnu traku Google Chrome-a, prikazuje mu se upozorenje koje je jasno istaknuto crvenom bojom. Korisnika se upozorava da se radi o adresi koja je prijavljena na tzv. crnu list (eng. *blacklist*). Google, kao i ostali proizvođači preglednika, na dnevnoj bazi nadograđuje listu potencijalno opasnih stranica. Pri svakom upisu adrese web stranice u adresnu traku preglednika, prvo se provjerava je li stranica na crnoj listi (jer već i pri samom učitavanju takvih stranica moguće je učitati i zlonamjerni kod) te o tome obavještava korisnika.



Slika 11. Prikaz upozorenja u Google Chrome-u

U upozorenju je jasno navedeno objašnjenje zašto je Chrome odbio pristupiti traženoj stranici. Također, ovaj alat omogućava korisniku provjeru stranice koju u budućnosti želi posjetiti. Ovu provjeru je moguće obaviti na adresi:

http://www.google.com/safebrowsing/diagnostic?site=

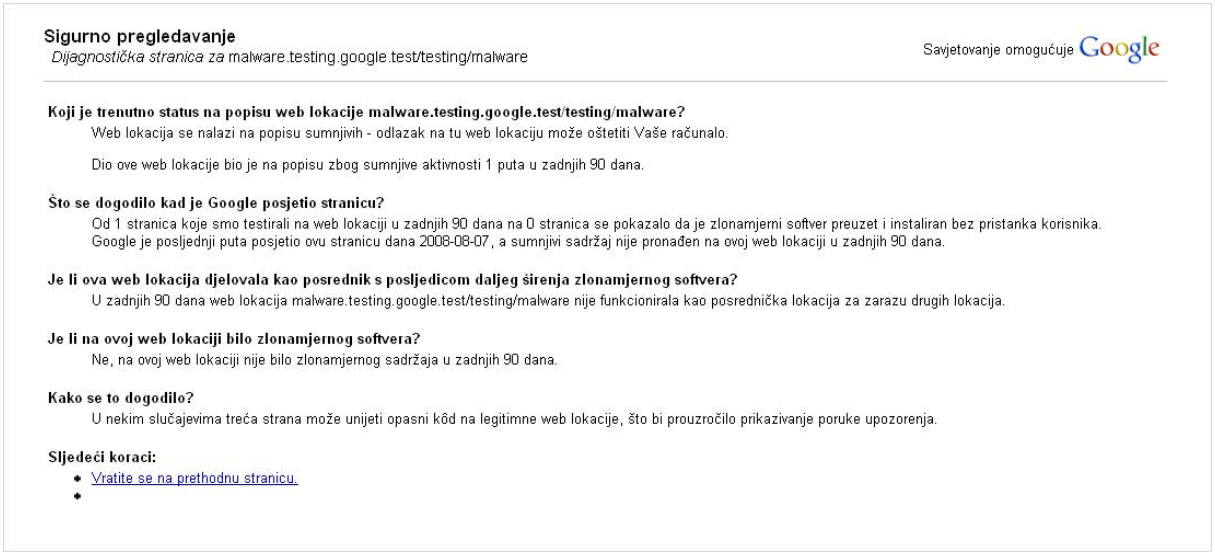
Provjera se obavlja tako da se nakon prethodno navedene adrese utipka adresa stranice koju korisnik želi posjetiti. Dakle upisano u adresnoj traci bi trebalo izgledati ovako:

http://www.google.com/safebrowsing/diagnostic?site=**ime_stranice**

Slika 12. Primjer načina provjere web stranica

Nakon unosa adrese, treba pritisnuti tipku „Idi na…“ kako bi se uputio zahtjev za pokretanjem dijagnostike za stranicu koju se provjerava. Ukoliko je stranica sigurna i ne nalazi se na crnoj listi zlonamjernih stranica, preglednik će izbaciti rezultate dijagnostike u kojima će pisati da je stranica sigurna. Međutim, ako se radi o stranici koja je prijavljena na crnu listu, preglednik će izbaciti upozorenje da se radi o takvoj stranici. Uz to, ispisati će cijeli niz statistika kao što su:

- broj sumnjivih ili zlonamjernih aktivnosti u zadnjih 90 dana,
- broj stranica u traženoj web adresi koje se smatraju sumnjivim ili zlonamjernim,
- radnja koja se odvila kada je Google posjetio web stranicu (preuzimanje zlonamjernih programa, krađa podataka, itd.),
- broj radnji koji se odvio,
- datum zadnje provjere
- i još nekolicinu zanimljivih podataka

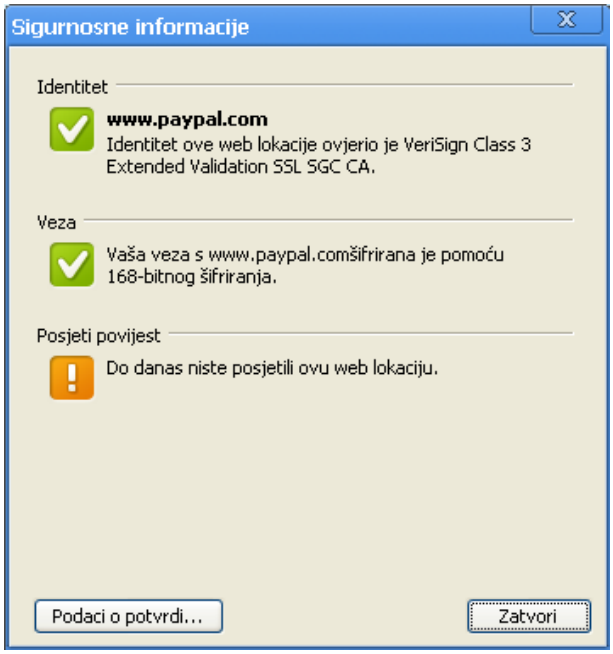


Slika 13. Primjer statistika Google-ove dijagnostičke web stranice

4.3. Alat za isticanje domene

Još jedna od zaštita je modul za isticanje domene Chrome preglednika. Alat radi tako da provjerava nalazi li se korisnik u stvarnoj domeni web stranice. Ovaj je alat prvenstveno namijenjen zaštiti od spoofing napada, tj. krivotvorenih web adresa. Stvarna je domena označena i istaknuta crnim slovima, a ostatak adrese je označen sivim tako da je korisniku lako uočiti koju je adresu zapravo posjetio.

Također, ovaj alat istovremeno obavlja provjeru autentičnosti tražene web adrese. Ako se radi o stranicama koje imaju neku vrstu certifikata kojim potvrđuju svoj stvarni identitet, alatna traka u pregledniku će poprimiti žutu boju (obično su to stranice poput PayPal-a, stranica na kojima se obavljaju novčane transakcije, itd.). U lijevoj strani alatne trake će se pojaviti maleni grafički simbol. Pritiskom lijeve tipke miša na taj simbol moguće je pročitati informacije o identitetu posjećene web stranice.



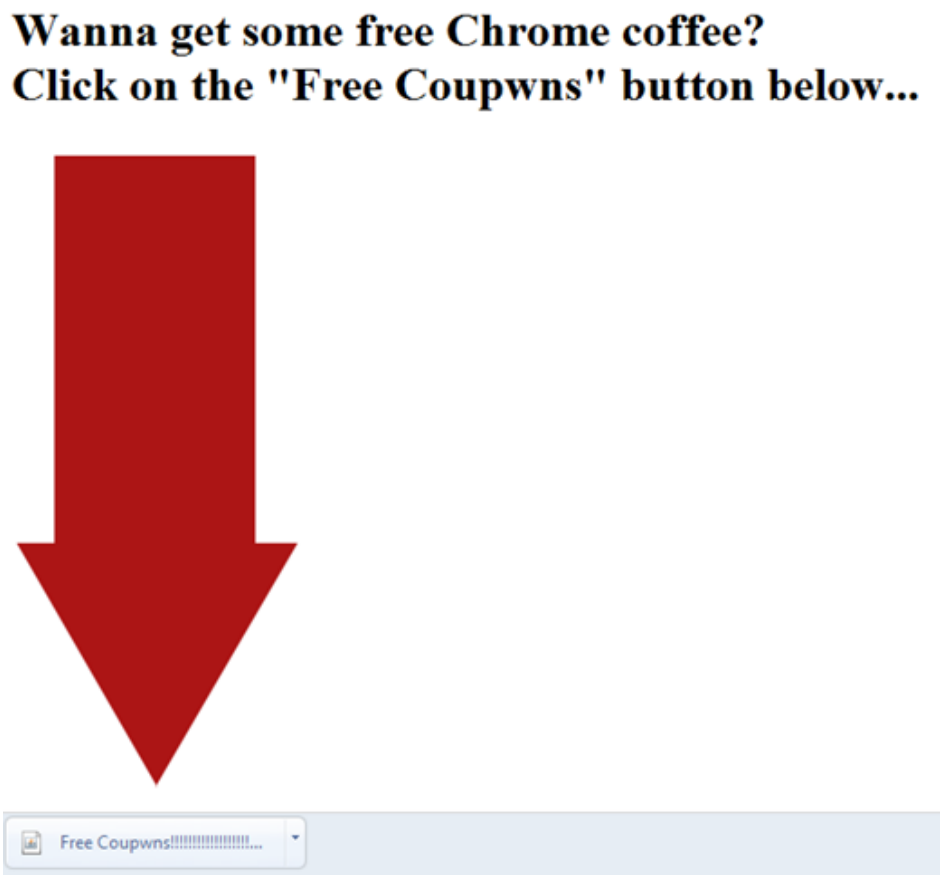
Slika 14. Podaci o identitetu posjećene web stranice

Kao što je vidljivo, u okviru dijaloga su navedeni podaci o tvrtki, certifikat kojim je ovjeren identitet stranice, je li veza između korisnika i stranice šifrirana i broj posjeta toj web stranici od strane lokalnog korisnika koji je postavio upit.

5. Sigurnosni propusti u Google Chrome beta

Samo dan nakon objave Google Chrome-a u javnost, pronađen je prvi veći sigurnosni propust. Uzrok je propust Webkit-a, pokretačkog dijela (eng. *engine*) Google Chrome-a. Ovaj je propust otprije poznat iz preglednika Safari koji se također temelji na Webkit-u. U pregledniku Safari je taj propust ispravljen, mnogo prije nego što je Chrome pušten u upotrebu. Propust u Chrome nije ispravljen jer on koristi stariju inačicu Webkit-a u kojem je taj propust još uvijek postojao. Korisnici koji nisu imali instaliranu Java komponentu, koja omogućuje pokretanje naprednih multimedijskih sadržaja, nisu bili ugroženi. Korisnici koji su istovremeno na računalu imali Chrome preglednik i Java komponentu su bili ugroženi. Ovaj propust se smatra opasnim, ali nije ga moguće pokrenuti udaljenim napadam, već je korisnik morao direktno sudjelovati. Ako korisnik preuzme Java datoteku koja je posebno namijenjena za tu radnju, datoteka se po preuzimanju sama pokreće i bez korisnikovog nadzora izvršava. Ovaj bi propust mogao učiniti znatnu štetu korisnicima Chrome-a jer omogućuje napadaču izvršavanje zlonamjernog koda i stjecanje najviše razine ovlasti na računalu.

Ovaj je propust otkrio i javnosti slikovito prikazao stručnjak za računalnu sigurnost Aviv Raff. Kako bi demonstrirao ozbiljnost i opasnost propusta, unutar web stranice je stavio dijaloški okvir za preuzimanje Java datoteke koja se po preuzimanju sama pokreće. Nakon što bi korisnik pokrenuo preuzimanje datoteke, stvari bi izmakle kontroli. Preuzeta datoteka bi bez znanja i dozvole korisnika izvršila zadanu akciju. Na sreću, u demonstraciji ovog propusta nije se radilo o datoteci koja je sadržavala zlonamjerni programski kod, već je samo pokretala program Notepad.



Slika 15. Stranica kojom je obavljena demonstracija propusta

Kako je ovaj propust objavljen, da stvari ne bi izmakle kontroli Google je bio prisiljen brzo reagirati i zaštititi korisnike od potencijalne opasnosti. Propust je ispravljen u vrlo kratkom roku i više nije moguće izvesti napad koristeći se ovim propustom.

Drugi pronađeni propust vezan je uz privatnost korisnika pri korištenju Chrome preglednika. Naime, svaki put kada korisnik utipka web adresu neke stranice u adresnu traku, ta adresa se šalje na Google-ove poslužitelje i tamo zapisuje. Chrome čak šalje i kolačiće na istu lokaciju. Problem je u tome što se utipkane web adrese i

kolačići zapisuju u Google korisnički račun korisnika, koji se povezuje s identitetom korisnika. Ovaj propust je opasan i zato jer napadač može presresti slanje kolačića i pregledavanih web stranica, a u krajnjem slučaju i ukrasti identitet.

Propust vezan uz upisivanje znaka "%" u adresnu traku se smatra pitanjem stabilnosti Chrome preglednika, ali ipak ga je korisno navesti. Upisivanje znaka „%" u adresnu traku dovelo je do pada preglednika, a u nekim slučajevima i cijelog računalnog sustava. Propust se može iskoristiti na slijedeći način:

1. korisnik pregledava Internet i na stranici koju pregledava se nalazi brza poveznica (eng. *hyperlink*)
2. u adresi te poveznice upisan je znak „%"
3. ako korisnik mišem prijeđe preko te poveznice, preglednik će se srušiti

Tvrtka za računalnu sigurnost Bach Koa Internetwork Security je otkrila još jedan potencijalno opasan propust. Radi se o propustu vezanom uz pohranjivanje web stranica s velikim zaglavljem na računalo. Ako bi korisnik pokušao pohraniti takvu stranicu na svoje računalo, preglednik bi se srušio. U zaglavlje stranica moguće je ubaciti zlonamjerni programski kod, stoga ovaj problem predstavlja veliku opasnost. Kada bi se dogodio slučaj da je u zaglavlje takve stranice ubačen zlonamjerni programski kod, rušenjem preglednika napadač bi stekao ovlasti na računalu korisnika i pokrenuo izvršavanje drugih proizvoljnih programskih kodova.

Uz navedene, pronađeno je još nekoliko sigurnosnih propusta koji su predstavljali manju opasnost. Svi od navedenih propusta su ispravljeni čime je smanjena mogućnost napada na korisnike ovog preglednika.

Kako bi se čitatelju zornije predočila sigurnost Chrome preglednika, u tablici 1dana je usporedba broja sigurnosnih propusta Chrome, IE i Firefox web preglednika.

Preglednik	Broj propusta	Broj kritičnih propusta	Udio na tržištu
Internet Explorer 8 beta	137	63	71.52 %
Mozilla Firefox 3	73	28	19.46 %
Google Chrome beta	11	3	0.78 %

Tablica 1. Usporedba Google Chrome-a sa ostalim preglednicima

6. Preporuke za korištenje Chrome preglednika

Zasad se ne preporučuje koristiti Google Chrome u poslovnom okruženju jer još uvijek nije u potpunosti siguran za upotrebu. Usporedbom broja propusta u pregledniku, vidljivo je da Chrome ima najmanji broj propusta. S druge strane, Chrome je novi preglednik na tržištu, tako da broj od 3 kritična propusta u kratkom vremenu predstavlja veliku opasnost. Upravo zbog činjenice da su u Chrome ugrađeni moduli iz više različitih preglednika, stručnjaci savjetuju korištenje drugih preglednika (bar dok ne se ne objavi *stable* inačica).

Pri korištenju preglednika potrebno je paziti na zlonamjerne web stranice koje se nalaze na Internetu. Svi moduli zaštite (SmartScreen filtar, alat za isticanje domene, itd.) i načini pregledavanja (InPrivate i Inkognito) su ugrađeni kako bi korisnika upozorili na zlonamjerne web stranice. Za potpunu zaštitu potrebno je primijeniti i oprez pri pregledavanju Internet sadržaja, jer napadači stalno nalaze nove načine provaljivanja u korisnička računala. Najopasniji su propusti vezani uz Javascript i ActiveX kontrole, pa većina korisnika treba posveti veliku pozornost na zaštitu od takvih sadržaja (blokiranjem Javascript-a i ActiveX kontrola).

Prednosti Google Chrome preglednika u odnosu na Mozilla Firefox i Internet Explorer su:

- veća brzina učitavanja sadržaja web stranica
- jednostavnije *user-friendly* sučelje
- minimalistički dizajn koji korisnicima omogućuje lakše snalaženje.

S druge strane, mane Google Chrome preglednika su:

- nedostatak statusne trake u pregledniku kako bi korisnik vidio što se učitava u preglednik
- nedostatak trake za pretraživanje
- nemogućnost primanja RSS (eng. *Rich Site Summary*) vijesti u pregledniku

Google je podbacio kada je u pitanju sigurnost Chrome-a u odnosu na Internet Explorer i Mozilla Firefox. Neki od kritičnih sigurnosnih propusta nisu smjeli dospjeti u javnost radi zaštite korisnika. Google će morati uložiti mnogo truda u zaštitu korisnika, jer u Chrome-u još uvijek postoji velik broj propusta koji nisu ispravljeni.

7. Predviđanja za „stable“ verziju

Upitno je hoće li Google Chrome preuzeti većinu korisnika koji su dosada koristili Internet Explorer ili Mozilla Firefox. Još uvijek dostupan jedino u beta izdanju, Chrome ipak polagano preuzima određen dio korisnika. Da li će postići planetarni uspjeh i udomaćiti se na računalu svakog korisnika pokazati će tek „stable“ verzija. Google još uvijek nije službeno najavio točan datum pojavljivanja pune (stable) verzije, jer kako je naglašeno, želi se postići maksimalna sigurnost.

Chrome je doživio veliki debakl jer je već nakon prvog dana pronađen ozbiljan i opasan sigurnosni propust. Međutim, sva ta potraga za propustima može rezultirati samo sigurnijim preglednikom, jer za svaki propust postoji i rješenje. Samo je pitanje koliko brzo i koliko kvalitetno će se uočeni propust ispraviti.

Stručnjak za računalnu sigurnost, Aviv Raff je slikovito opisao Google Chrome:

> „U prirodi, kada pomiješate dvije različite vrste, dobijete hibrid. U svijetu preglednika, kada uzmete Mozilla Firefox ili Internet Explorer i pomiješate ih s preglednikom Safari, dobijete Google Chrome.“

Vrlo kritičan komentar za Chrome može se pokazati i istinitim izlaskom „stable“ verzije. Google je stvorio Chrome tako da je pomiješao zajedno više različitih funkcionalnosti drugih preglednika, što je vrlo problematično kada je u pitanju sigurnost pri korištenju preglednika. Google će morati otkriti sve propuste u drugim preglednicima čije je dijelove ugradio u Chrome, a potom i u samom Chrome-u. Ti će propusti, pretpostavlja se, biti ispravljeni tek nakon što budu javno objavljeni. To bi značilo da bi korisnici duže vrijeme mogli biti nezaštićeni.

Google Chrome je zapravo preuzeo neke od propusta iz drugih preglednika. Niti jedan od tih propusta ne predstavlja veliku opasnost pojedinačno, ali kada ih se sve pomiješa zajedno, javljaju se veliki problemi. Jedan od problema je također automatsko aktualiziranje preglednika bez znanja korisnika. Iako se funkcija čini korisnom, neki su se korisnici javno bunili zbog aktualiziranja bez njihovog znanja. Skup malih problema čini jedan veliki problem.

Gotovo svi stručnjaci predviđaju loš odaziv korisnika po izlasku „stable“ verzije, no potrebno je saslušati i korisnike. Veliki dio korisnika s oduševljenjem čeka izlazak „stable“ verzije, a da li će opravdati njihova očekivanja preostaje za vidjeti.

8. Zaključak

Google Chrome je zasigurno novost na tržištu preglednika. Predstavljena su neka nova rješenja koja su ugrađena u Chrome, što je izazvalo veliki interes javnosti. Očekivanja su bila velika, a rezultati loši. Google je najavio pokretanje revolucije izlaskom Chrome-a, a postigao je vrlo malo. Chrome uistinu zadivljuje minimalističkim izgledom, jednostavnošću i brzinom. Da bi bio što jednostavniji za korištenje, čak su maknuti i neki, kako je Google rekao, „nepotrebni gumbi".

Pokazalo se da je većini korisnika sigurnost na prvom mjestu, a to se smatra područjem u kojem je Chrome zakazao. Opasni propusti nedugo poslije izlaska beta verzije u javnost su odvratili dio korisnika. Stručnjaci za računalnu sigurnost tvrde da korisnici još dugo vremena neće moći biti potpuno sigurni u Internet okruženju ako budu koristili Chrome.

Beta verzije programa su testne verzije i često ih je riskantno koristiti, naročito u okruženju poput Interneta, gdje je potrebna najviša razina sigurnosti. Na Google Chrome-u se stalno radi, beta verzija je aktualizirana čak pet puta u zadnjih mjesec dana što je dokaz napora i truda koji Google-ovi razvojni inženjeri ulažu u ovaj preglednika. U „stable" verziji će sve biti poznato, tako da se savjetuje pričekati stabilnu, sigurnu i učinkovitu verziju preglednika Chrome i onda donijeti konačnu ocjenu.

9. Reference

[1] Secunia, izvješće o broju sigurnosnih propusta u preglednicima, http://secunia.com/, listopad 2008.

[2] Statistike o najčešće korištenim web preglednicima tvrtke Net Applications, http://marketshare.hitslink.com/report.aspx, listopad 2008.

[3] InPrivate pregledavanje, http://www.microsoft.com/windows/internet-explorer/beta/features, listopad 2008.

[4] SmartScreen filtar, http://www.microsoft.com/windows/internet-explorer/beta/features, listopad 2008.

[5] Sigurnost preglednika Mozilla Firefox, http://www.mozilla.com/en-US/firefox/features/#security, listopad 2008.

[6] Poznati sigurnosni propusti Mozille Firefox 3, http://www.mozilla.org/security/known-vulnerabilities/firefox30.html, listopad 2008.

[7] Svojstva Google Chrome-a, http://www.google.com/chrome/intl/hr/features.html#, listopad 2008.

[8] Java propust u Google Chrome-u, http://aviv.raffon.net/2008/09/03/GoogleMule.aspx, rujan 2008.

[9] Baza znanja Google Chrome-a, http://chromekb.com/vulnerabilities/, listopad 2008.

[10] Google Chrome izdanja, http://googlechromereleases.blogspot.com/, listopad 2008.

[11] Google Chrome, http://www.siliconrepublic.com/news/article/11357/, rujan 2008.