



Univerzitet Singidunum
Departman za poslediplomske studije
Savremene informacione tehnologije

Željko Radnov

Veb brauzeri i zlonameran softver

- Master rad -



Beograd, 2011.

Univerzitet Singidunum
Departman za poslediplomske studije
Savremene informacione tehnologije

Veb brauzeri i zlonamerni softver

- Master rad -

Profesor:
Prof. dr Mladen Veinović

Student:
Željko Radnov



Beograd, 2011.

Sažetak

U ovom master radu izvršena je komparativna analiza uspešnosti pet veb brauzera pri otkrivanju i blokiranju širenja zlonamernog softvera. Koriste se testovi kompanija za Internet bezbednost. Analiza je usmerena na izbor veb brauzera koji ima najbolje alate za zaštitu korisnika od zlonamernog softvera. U radu su prikazane karakteristike alata za zaštitu od zlonamernog softvera kod primenjenih veb brauzera. Detaljno su razmatrane tehnike za sprečavanje napada. Analiziraju se najčešće vrste zlonamernog softvera i tehnike upada u računar preko brauzera. Poslednji deo rada predstavlja uticaj Internet kriminala. Data su predviđanja razvoja zlonamernog softvera i njegov uticaj na nove Internet tehnologije i predstojeće alate za nove verzije brauzera.

Ključne reči: zlonameran softver, brauzer, alati, virus, pecanje, drive by-download

Abstract

In this Master's Thesis the comparative analysis of the effectiveness of five Web browsers for detecting and blocking the spread of malicious software is completed. It uses tests of companies for Internet security. The analysis is focused on the selection of a web browser that has the best tools to protect users from malicious software. The paper also describes the characteristics of tools to protect against malicious software with the use of web browsers. Techniques for preventing the attacks are discussed in detail. The last part of paper represents the impact of Internet crime. Given the anticipated development of malware and its impact on new Internet technologies and the upcoming tools for the new versions of the browsers.

Key words: malware, browser, tools, virus, phishing, drive by-download

Sadržaj

Uvod	7
1. Metologija istraživačkog rada	8
1.1 Uvodne napomene i obrazloženje rada	8
1.2 Predmet istraživanja	8
1.3 Ciljevi i zadaci istraživanja	8
1.4 Istraživačke hipoteze.....	8
1.5 Metodi istraživanja i tok istraživačkog procesa	9
2. Definicija zlonamernog softvera	10
3. Istorijat veb brauzera	11
4. Mozilla Firefox	12
4.1 Ukratko.....	12
4.2 Napadi , prevencije i alati.....	12
4.2.1 Napadi	12
4.2.2 Prevencije i alati.....	13
5. Opera	15
5.1 Ukratko.....	15
5.2 Napadi , prevencije i alati.....	15
5.2.2 Napadi	15
5.2.3 Prevencije i alati.....	15
6. Apple Safari	17
6.1 Ukratko.....	17
6.2 Napadi , prevencije i alati.....	17
6.2.1 Napadi	17
6.2.2 Prevencije i alati.....	17
7. Internet Explorer	19
7.1 Ukratko.....	19
7.2 Napadi , prevencije i alati.....	19
7.2.1 Napadi	19
7.2.2 Prevencije i alati.....	20
8. Google Chrome	22
8.1 Ukratko.....	22
8.2 Napadi , prevencije i alati.....	22
8.2.1 Napadi	22
8.2.2 Prevencije i alati.....	22
9. Istorijat zlonamernog softvera	24
10. Vrste zlonamernog softvera	25
10.1 Virusi.....	26
10.2 Trojanci	26
10.3 Računarski Crv	26
10.4 Crimeware	27
10.5 Scareware	27
10.6 Rootkits	27
10.7 Backdoors.....	27
10.8 Ransomware	28
10.9 Potencijalno nepoželjni softver	28

10.9.1 Spyware	28
10.9.2 Zlonamerni adware.....	28
10.9.3 Dialer.....	28
10.9.4 Administratorski alat za daljinsko korišćenje.....	28
10.9.5 Provaljivač lozinki	28
10.9.6 Joke – šala.....	28
11. Vrste napada na veb brauzere, strategije i tehnike odbrane	29
11.1 Socijalna manipulacija	29
11.1.1 Phishing – pecanje.....	29
11.1.1.1 Napadi.....	30
11.1.1.2 Izmena linka	31
11.1.1.3 Falsifikovanje sajtova	31
11.1.2 Anti-phishing – anti-pecanje.....	32
11.1.2.1 Socijalni pristup.....	32
11.1.2.2 Zakonodavni pristup	32
11.1.2.3 Tehnološki pristup.....	33
11.2 Drive-by download	35
11.2.1 Implementacija tehnike za otkrivanje napada preko	36
drive-by download metode.....	36
11.2.1.1 Efikasnost tehnike	36
11.2.1.2 Optimizacija performansi	37
12. Uloga organizovanog kriminala i finansijski aspekt.....	38
12.1 Botnet	38
12.2 Finansijski aspekt.....	38
13. Predviđanja širenja i razvitka zlonamernog softvera	40
14. Uticaj zlonamernog softvera na Veb 2.0	43
14.1 Veb 2.0	43
14.2 SSL enkripcija	43
14.3 Pecanje preko HTML-a.....	44
14.4 Cross site scirpintg (XSS)	44
14.5 Third-party aplikacije i socijalna manipulacija kod Facebook-a.....	44
15. Komparativna analiza pet veb brauzera	46
15.1 Prvi test – socijalna manipulacija	46
15.2 Drugi test – socijalna manipulacija.....	47
15.3 Treći test – socijalna manipulacija.....	48
15.4 Četvrti test – socijalna manipulacija	49
15.5 Test na metodu pecanja	50
Zaključak.....	50
15.6 Istraživački rad.....	50
16. Pravci istraživanja kod predstojećih verzija brauzera	52
16.1 Mozilla Firefox.....	52
16.2 Opera.....	52
16.3 Apple Safari.....	52
16.4 Internet Explorer.....	52
16.5 Google Chrome.....	53
Zaključak	54
Literatura.....	55

Uvod

Širenje zlonamernog softvera vrši se zloupotrebom ranjivih sigurnosnih delova brauzera – tehnika *drive-by download* i socijalnom manipulacijom korisnika, gde je najrasprostranjenija tehnika pecanje. Prvih nekoliko godina štetnog softvera označavalo je isključivo širenje preko elektronske pošte i to su uglavnom bili virusi i računarski crvi. Prve viruse su stvarali programeri entuzijasti koji su želeli da se dokažu i cilj ovakvog delovanja nije bio novac. Kasnije, kada se broj korisnika Interneta povećao zahvaljujući boljoj infrastrukturi i ubrzanju konekcija došlo je do evolucije štetnih programa. Napadi su sve manje bili organizovani preko elektronske pošte, a sve više preko veb brauzera. Programeri su se počeli udruživati u grupe zarad stvaranja boljih i za otkrivanje težih štetnih programa i razvijanja sve boljih tehnika upada u računare kako običnih korisnika tako i u sisteme kompanija. Ljudi iz organizovanog kriminala su vremenom preuzimali usluge profesionalaca, jer su uvideli mogućnost ogromne zarade koju ovakav softver omogućava. Prvih godina Interneta postojala su u suštini samo dva dok danas postoji pet glavnih brauzera i stoga napadači imaju veći izbor pri stvaranju nekih tehnika širenja zlonamernih programa.

U ovom master radu prikazane su karakteristike svih brauzera pojedinačno pri otkrivanju i sprečavanju zlonamernog softvera. Prvih nekoliko poglavlja obuhvata određene vrste napada za svaki brauzer i alate koje oni poseduju. Sledeći deo rada pripada zlonamernom softveru uopšte – istorijat i vrste zlonamernog softvera kao što su virusi, crvi, rooktitsi, potencijalno nepoželjan softver itd. Naredno poglavlje prikazuje tehniku socijalne manipulacije - pecanje i tehniku iskorišćavanja ranjivosti memorije brauzera – *drive by download*. Takođe uključuje i nekoliko vrsta pristupa za sprečavanje pecanja i jednu tehniku koja se može implemetnirati u brauzer i blagovremeno otkriti napad preko tehnike *drive-by download*.

Sledećih nekoliko poglavlja predstavlja ulogu organizovanog kriminala u stvaranju i distribuiranju zlonamernog softvera, nekoliko predviđanja razvoja zlonamernog softvera i njegov uticaj na nove tehnologije na Internetu. Pretposlednje poglavlje uključuje nekoliko testova svih pet brauzera pri otkrivanju tehnika socijalne manipupulacije i rezultate. Poslednje poglavlje bavi se novim alatima protiv zlonamernog softvera u predstojećim verzijama svih pet brauzera.

1. Metodologija istraživačkog rada

1.1 Uvodne napomene i obrazloženje rada

Rad predstavlja pet brauzera i njihovu moć u otkrivanju i sprečavanju zlonamernog sa jedne strane, dok sa druge prikazuje sve vrste zlonamernog softvera pojedinačno, tehnike kojima se hakeri udruženi u Internet kriminal služe da bi zlonamerni softver preko brauzera nelegalno ubacili u računare. Opisane su i tehnike i različiti pristupi za sprečavanje zlonamernog softvera, finasijski aspekt Internet kriminala, uticaj ovakvog softvera na nove Internet tehnologije, nekoliko opsežnih testova koji mere uspešnost brauzera protiv zlonamernog softvera i na kraju nove alate brauzera u predstojećim verzijama.

1.2 Predmet istraživanja

Predmet rada su bili brauzeri i zlonamerni softver. Prikazana je čvrstina njihove zaštite od zlonamernog softvera radi što bezbednijeg korišćenja. Prikazani su prednosti i nedostaci posebnih karakteristika koje sami brauzeri poseduju kao što su alati koji služe da otkriju i spreče upad zlonamernog softvera na računar i najčešće vrste napada na pojedinačne brauzere. Opisane su vrste zlonamernog softvera, njihove karakteristike, tehnike upada u računar koje hakeri koriste i tehnike sprečavanja takvih upada. Poslednji deo rada čine uticaji zlonamernog softvera na nove Internet tehnologije, finasijski aspekt i uticaj Internet kriminala i spremnost razvojnih timova brauzera na stvaranje novih alata u predstojećim verzijama prikazanih brauzera.

1.3 Ciljevi i zadaci istraživanja

Rad je namenjen kako iskusnijim korisnicima računara koji se profesionalno bave zaštitom i bezbednosnim rizicima na mreži tako i najobičnijim kućnim korisnicima kojima je važno da bezbedno koriste Internet. Cilj rada je da pokaže koliko su u suštini brauzeri današnjice bezbedni, kako se snalaze njihovi razvojni timovi u borbi protiv zlonamernog softvera i da se prikaže koliko je uticaj zlonamernog softvera na informatičku industriju.

1.4 Istraživačke hipoteze

Opšta hipoteza

U početnim verzijama svih brauzera koji su opisani u ovom istraživanju postojala je vrlo slaba (kod nekih nikakva) zaštita od zlonamernog softvera. Nedovoljna istraženost u oblasti bezbednosti i slaba razvijenost alata koji se ugrađuju u brauzere ključni su razlog sve većeg broja oštećenih korisnika.

Značajna je opasnost zlonamernih programa kako na kućne korisnike koji Internet koriste za socijalno umrežavanje, multimediju i plaćanje usluga tako i na poslovne korisnike čije poslovanje dosta zavisi od bezbednog Interneta.

Radna hipoteza

Napredak počinje novijim verzijama programa gde se ispravljaju sigurnosne greške prethodnih verzija, poboljšavanju njihovih alata specijalizovanih za borbu protiv štetnog softvera i stvaranje organizacija i grupa koji istražuju Internet u potrazi za inficiranim stranicama. Brauzeri se preko servera povezuju sa podacima ovih grupa i snimaju crne liste (spisak potencijalno opasnih stranica).

Pojavom sve većeg broja štetnog softvera, sve je više istraživanja na tu temu, više antivirusnih kompanija, organizovanih grupa koji pružaju podatke o kriminalnim grupama koje stvaraju i šire zlonamerne programe itd. Implementacije raznih tehnika za otkrivanje zlonamernog softvera koji dolazi preko brauzera ili elektronske pošte i donošenjem dobrih i primenjivih zakona doprinosi određenim vidljivim rezultatima u sprečavanju pojave i širenja ove vrste softvera.

1.5 Metodi istraživanja i tok istraživačkog procesa

Metodologija istraživanja je bila u okviru korišćenja Interneta i pretrage za tekstovima, dokumentima i blogovima raznih IT stručnjaka i kompanija koje se bave tematikom bezbednosti korisnika na Internetu. Informacije su izvučene i od nekoliko istraživanja koja su detaljno obuhvatala najčešće vrste napada na brauzere. Sve informacije su proverene na više mesta da bi se pokazala verodostojnost i važnost.

2. Definicija zlonamernog softvera

Zlonameran softver je softver dizajniran tako da bez znanja korisnika ili prevarom korisnika inficira tj. upadne u njegov računar. Na engleskom *malicious softver* – *malware* se stvara od strane hakera, pojedinačno ili grupno u cilju diskreditovanja korisnika, krađe njihovih važnih podataka kao što su na primer lozinka i korisničko ime računa u banci i broj kreditne kartice, prebacivanje sa reklama na inficirane stranice, nekontrolisano iskakanje prozora sa reklamama nepostojećih programa itd. U suštini novac je glavni pokretač.

Zlonameran softver uključuje kompjuterski virus, trojance, računarske crve, spajvere i druge vrste neželjenog softvera. Neki program se definiše kao zlonameran više prema namerama njegovih kreatora nego prema specifikacijama i karakteristikama. Zlonamernim softverom se ne smatra na primer neki program koji ima legitimnu funkciju, ali i grešku – *bug*.

Zlonamerni programi su dobro napravljeni programi sa lošom namerom.

U suštini postoje dva načina pomoću kojih napadači pokušavaju da ubace svoj zlonameran softver:

- Drive-by download

Ova vrsta napada jedna je od najčešćih metoda širenja zlonamernih programa. Vršiti se isključivo bez znanja korisnika. Obično se zloupotrebljavaju ranjivost memorije brauzera i njegovi plug-in-ovi da bi se aktivirao *Shellcode*. *Shellcode* je mali deo koda koji aktivacijom ubacuje zlonameran program u brauzer tj. operativni sistem korisnika.

- Social engineering – socijalna manipulacija

Ovo je vrsta manipulacije korisnika da bi izvršili neke radnje ili pružili osetljive informacije, pre nego što bi se pristupilo nekoj tehnici upada u računar korisnika. Ovo je ključna razlika između ovog načina širenja zlonamernog softvera i Drive-by download tehnike, jer ovde korisnik svesno učitava stranicu. Ovde spadaju pecanje, namamljivanje, izmena teksta (*Pretexting*) i drugi.

Pecanje – *Phishing* predstavlja najrasprostranjeniji način širenja zlonamernog softvera i uključuje neželjenu poštu – *spam*, lažiranje sajtova radi krađe novca preko kreditnih kartica i preuzimanja ostalih osetljivih podataka.

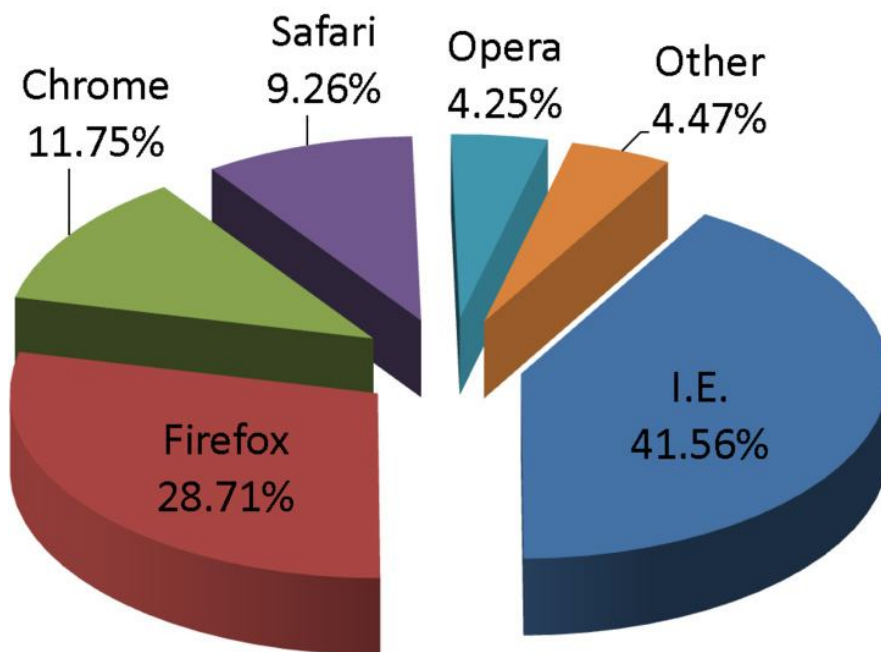
3. Istorijat veb brauzera

Tim Berners – Lee je osnivač WorldWideWeb-a, sistema povezanih hipertekst dokumenata kojima se pristupa preko Interneta. On je 1991. godine dizajnirao prvi program za pretraživanje takvog sistema, brauzer nazvan Nexus. Dve godine kasnije je nastao Mosaic, brauzer sa jednostavnim interfejsom i lakom instalacijom i postao je uzor za kasnije brauzere. 1994. godine Mark Andreessen, vodeći programer u razvoju Mosaic-a napušta taj projekat i osniva kompaniju Netscape i sa njom veb brauzer Netscape Navigator.

Nakon godinu dana Microsoft je izbacio prvu verziju Internet Explorera i zahvaljujući jednostavnosti brauzera i velikom procentu zastupljenosti operativnog sistema Windows, IE postaje dominantan na tržištu brauzera. Opera se pojavljuje godinu dana kasnije i uprkos nekim svojim originalnim opcijama do danas ostaje brauzer sa vrlo malim procentom korišćenja.

Kompanija Apple je 2003. predstavila svoj brauzer Safari.

1998. godine Netscape prelazi na otvorenu platformu *open source* i projekat nazvan Mozilla kasnije prelazi u organizaciju iz koje izlazi novi brauzer prvobitno nazvan Phoenix, zatim Firebird, da bi na kraju bio preimenovan u Firefox i prva finalna verzija je izašla 2004. godine.



Grafikon 1.0 - Upotreba brauzera za mesec januar 2011. (izvor Wikimedia)

4. Mozilla Firefox

4.1 Ukratko

Ovaj brauzer je formiran od strane Mozila Fondacije i potpuno je otvoren tj. aplikacija je open source izdata pod GPL licencom. To znači da je besplatan i da je svaki deo aplikacije slobodan da se čita, uređuje i proučava. Njegov osnovni pokretač (engine) je Gecko. Po broju korisnika nalazi se na drugom mestu sa oko 23%. Razvija se za Microsoft Windows, GNU/Linux, FreeBSD, OpenSolaris, MAC OSX i mnoge druge unix-olike operativne sisteme.

4.2 Napadi , prevencije i alati

Kao drugi brauzer po broju korisnika, za Firefox postoji veliki broj zlonamernih programa. Njegova prednost je to što je otvorenog koda pa se može lako proučavati od strane univerziteta, raznih laboratorija koje se bave sigurnosnim problemima na Internetu, pojedinaca programera koji dobrovoljno otkrivaju greške u samom brauzeru itd. Svi oni svojim istraživanjem mogu lako uputiti razvojni tim Mozille da za sledeću podverziju programa sprema rešenje za određeni bug (grešku) ili sigurnosnu rupu. Njegova mana je takođe otvoreni kod, jer ga mogu proučavati zlonamernici koji na razne načine mogu stvoriti neki štetan program upravo i samo za Firefox korisnike. Jedna od karakteristika Firefox-a je ima mogućnost proširenja u vidu ekstenzija (dodataka), koji će se u budućnosti zvati Firefox apps. Te ekstenzije povećavaju opcije brauzera i olakšavaju mnoge radnje na Internetu (provera mail-a, skidanje fajlova, upravljanje multimedijom, pretraživanje itd). Upravo su ekstenzije napravile priličan problem programerima iz Mozille.

4.2.1 Napadi

U februaru 2010. godine Mozilla je priznala da nije temeljno izvršila sigurnosne provere na dve ekstenzije i inficiralo se oprilike 4,600 računara sa operativnim sistemom Microsoft Windows. Ekstenzije su bile eksperimentalnog tipa i sadržale su Trojanac koji se aktivirao kad je Firefox startovan. Zvale su se Sothing Web Video Downloader i Master Filer. Prva je imala trojanac Win32.LdPinch.gen, a druga Wun32.Bitfroze. Samim uklanjanjem ovih dodataka neće se obrisati Trojanac iz sistema nego se u pomoć mora pozvati neki od antivirusnih programa.

Još jedan zanimljiv slučaj desio se tokom 2009. godine kada su se pojavila dva zlonamerna programa. Prvi se zvao Firesox i nije bio samo rezultat Mozilline neobazrivosti, jer su sve aplikacije bile ranjive. Samo je najveća meta bio Firefox, verzija 3.07. On je bio u vidu plug-in-a i menjao je rezultate pretrage kroz sajtove Google, Altavista, Yahoo, MSN, Teoma, Ask, Pricegrabber i druge.

Drugi se zvao Foxicle i takođe je bio u vidu plug-in-a, ali radio je nešto sasvim drugo. Umesto instalacije samo odgovarajućeg programa za strimovanje pesama preko Interneta, on je ubacio i dodatak koji je nakon instalacije izbacivao iskačuće prozore sa reklamama. Tokom 2008. godine desio se još jedan napad na Firefox. Zvao se Chromeinject i ubacivao se u brauzer u vidu dodatka (ekstenzije) i krao lozinke i korisnička imena pri posećivanju sajtova gde se obavljaju novčane transakcije kao što su PayPal i drugi. Informacije su završile na udaljenom serveru u Rusiji gde su napadači preuzimali šifre i prebacivali (krali) novac sa korisničkih računa.

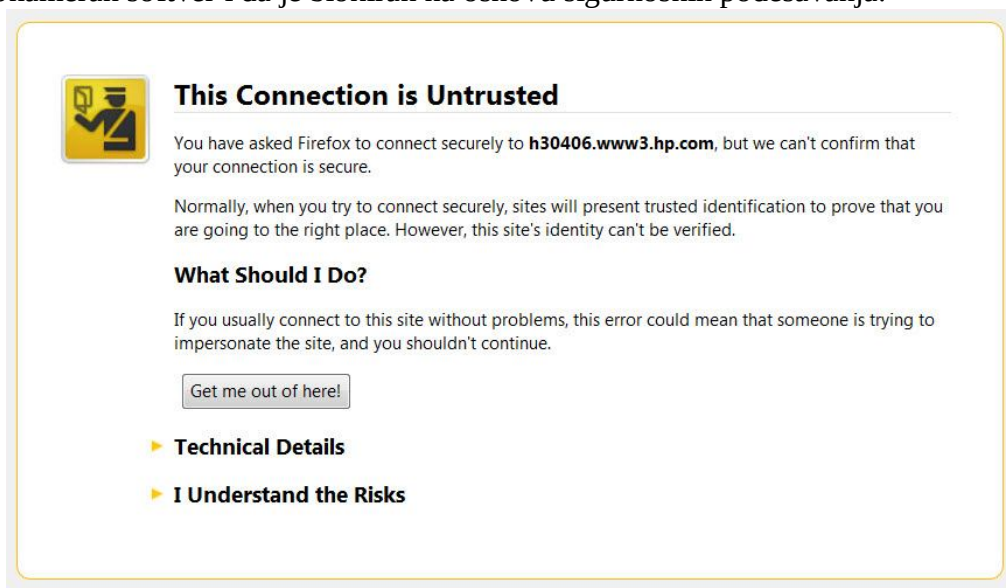
Pri istraživanju, tačnije pri pretrazi na sajtu www.google.com naišao sam na potencijalno inficiranu stranicu. Traženi pojam na sajtu www.google.com je bio *malware.pdf* i poslednji link na petoj stranici pretrage vodio je ka sledećoj stranici:

<https://wwwse.inf.tu-dresden.de/wiki/images/f/f6/PRO-TimLackorzynski.pdf>

Kao i u celom istraživanju koristio sam Firefox i on je prikazao upozorenje da stranica nije sigurna, tj. da server tog linka koristi nevažeći sertifikat. Takođe, svi ostali brauzeri su pri pokušaju učitavanja ovog linka izbacili svoje upozorenje.

4.2.2 Prevencije i alati

Od verzije 2.0 Firefox je imao specijalizovani alat za zaštitu od pecanja (phishing). Od verzije 3.0 poseduje novi alat protiv štetnog softvera koji detektuje inficiranu stranicu i sprečava njeno učitavanje. Kada se korisnik slučajno uputi ka takvoj stranici izlazi upozorenje da je to sajt koji sadrži zlonameran softver i da je blokiran na osnovu sigurnosnih podešavanja:



Slika 1.0 - Upozorenje za Firefox korisnika pri pristupu potencijalno inficiranog sajta

Kao i prethodni alat u verziji 2.0 i ovaj se takodje oslanja na listu (crnu listu) štetnog softvera stvorenu od strane Google Inc., kompanije za pretraživanje Internet stranica. Crna lista se stvara preko testova sajtova koje Google izvršava. Neki kriterijumi po kojima određene stranice zaslužuju mesto na crnoj listi su bazirani na istraživanju grupe StopBadware.org, stvorenu od Google-a, grupe Lenovo Group i Sun Microsystems Inc.

Svaki od ovih štetnih programa se mogu dobrom implementacijom sigurnosnih tehnika sprečiti. IT stručnjaci iz Secure Systems Lab-a, tehničkog univerziteta u Beču su stvorili jednu vrstu tehnike čiji je cilj da pronade zlonameran softver pre nego što se on aktivira. Svoje istraživanje su radili isključivo na Firefox-u, jer je njegov kod u potpunosti otvoren. Jedan od najtipičnijih načina širenja zlonamernog programa je preko Drive-by download-a i stoga je ova tehnika implementirana analizirajući taj način. Više o ovoj tehnici biće u drugom pristupnom radu.

5. Opera

5.1 Ukratko

Opera je stvoren od kompanije Opera Softver. Prva verzija je nastala 1996. godine, a trenutna verzija je 10.63. Ovaj brauzer je prvi koji je imao tabove (jezičke) u okviru jednog otvorenog prozora za razliku od drugih gde je za svaku stranicu morao biti otvoren po jedan prozor. Bez obzira na to do danas je relativno mali broj korisnika Opere. Osnovni pokretač je Presto. Verzije izlaze za Microsoft Windows, GNU/Linux, MAC OSX i FreeBSD.

5.2 Napadi, prevencije i alati

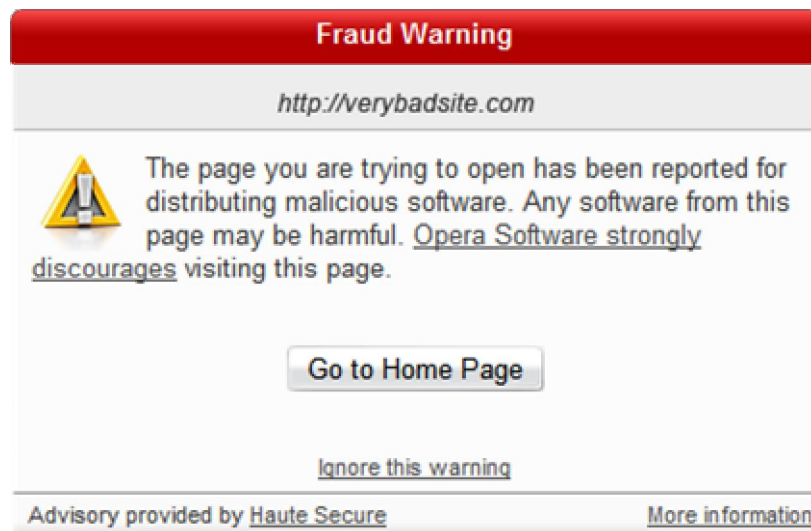
Opera, kao relativno slabo zastupljen među korisnicima nema puno štetnih programa pravljenih isključivo za njega, ali to ne znači da ne postoje. Ionako većina zlonamernih programa danas su pravljeni tako da napadaju sve brauzere.

5.2.2 Napadi

Jedan od zabeleženih napada na Operu je ubacivanje opasnog koda koji je omogućavao napadaču da utiče na neaktiviranu memoriju brauzera što je dovodilo do gašenja programa. U verziji 10.53 program je osvežen i problem je rešen.

5.2.3 Prevencije i alati

Razvojni timovi Opere su od serije 9, tačnije od verzije 9.1, implementirali alate protiv zlonamernog softvera (Malware Protection) i pecanja (Fraud Protection). Fraud Protection sadrži tehnologije iz GeoTrust-a, vodećeg dostavljača digitalnih sertifikata i PhishTank, kompanije za istraživanje podataka o pecanju na Internetu. Kada su oba alata aktivirana, kontaktira se server Opere po jednom za svaku stranicu koju korisnik poseti. HTTP sajtovi se proveravaju kroz zaštićen kanal, dok IP adrese u lokalnom intranetu neće biti proveravane. Onda se šalje ime domena na server koji proverava crne liste vezane za pecanje stvorene od kompanija Netcraft i PhishTank i crne liste vezane za zlonamernan softver stvorene od kompanije Yandex. Ako se ime domena složi sa imenom sa crne liste, server vraća XML dokument brauzeru opisujući mu tip problema (pecanje ili zlonamernan softver) i dodaje crnoj listi taj domen. Ime zatražene stranice naći će se u XML dokumentu i onda će brauzer prikazati korisniku upozorenje:



Slika 1.1 - Upozorenje za korisnika Opere pri pristupu potencijalno inficiranog sajta

Od verzije 9.5, Opera donosi novi sistem za zaštitu od zlonamernog softvera oslanjajući se na Haute Secure, kompaniju za Internet sigurnost iz Sijetla, osnovanu od strane bivših zaposlenih u Microsoft-u. Svakodnevno povezivanje ove verzije brauzera sa serverima ove kompanije radi osvežavanja liste sa opasnim sajtovima slično je kao i za prethodnu verziju.

6. Apple Safari

6.1 Ukratko

Safari je brauzer do skora pravljen isključivo za MAC OSX operativni sistem, jer se razvija od strane korporacije Apple koja stvorila ovaj operativni sistem. Osnovni pokretač je WebKit. Prva verzija van MAC OSX-a je izašla 2007. godine, dok je prva verzija uopšte 2003. godine. Četvrti je po udelu korišćenja. Razvija se za MAC OSX i Microsoft Windows.

6.2 Napadi , prevencije i alati

Prema mnogim analizama i istraživanjima ovaj brauzer ima solidan uspeh u sprečavanju opasnih programa, ali razvojni timovi često ostavljaju korisnike dugo bez zaštite, jer ne osvežavaju redovno ugrađene alate.

6.2.1 Napadi

Safari od svih brauzera ima najslabije alate za zlonameran softver i pecanje. Organizacije protiv zlonamernog softvera StopBadware.org, Lenovo Group i Sun Microsystems su tokom 2008. u više navrata pozivali kompaniju Apple da osveži svoj brauzer i zaštiti svoje korisnike od napada. Sugerisali su da opcija da korisnici ne budu upitani da li da snime na svoj računar neke vrste fajlova nije dobra i da se to mora promeniti. Istraživač za bezbednost i koautor knjige „Alati za mrežnu bezbednost“ Nitesh Dhanjani je u svom blogu upozorio da je Safari laka meta za napade hakera. Nepostojanje korisničke dozvole da se snimaju fajlovi mogu lako iskoristiti napadači da ubace opasni kod koji bi doveo veliki broj zlonamernog softvera na korisnikov računar. Nakon toga Dhanjani je poslao bezbednosnom timu Apple-a da zahtev da nešto urade po tom pitanju, a u odgovoru je stajalo da nepostojanje takve opcije nije sigurnosni problem.

6.2.2 Prevencije i alati

Tek od verzije 3.2 je počelo nešto da se menja po pitanju sigurnosti i to samo sa alatom protiv pecanja.



Slika 1.2 - Upozorenje za Safari korisnika pri pristupu potencijalno inficiranog sajta

Kasnije se pokazalo da je Apple požurio sa integriranjem njegovog alata u brauzer, jer je bio nedovršen. Nisu svi testovi temeljno izvršeni niti sva istraživanja sprovedena. Opcije koje se tiču alata su nedovoljne i dokumentacija na oficijelnom sajtu ne pruža nikakve informacije o tome kako alat uopšte funkcioniše. Na nekoliko testova je utvrđeno da sam alat ne pruža dovoljno dobru zaštitu od inficiranih stranica. Nekoliko sajtova koji su testirani od Mozille kao opasni Firefox je prikazivao upozorenje, dok je Safari bez upozorenja otvorio stranicu, a ista stvar se dogodila i sa stranicama specijalno kreiranih za druge brauzere.

7. Internet Explorer

7.1 Ukratko

Internet Explorer (u nastavku IE) je nastao 1995. godine kao deo paketa PLUS! za Windows 95 operativni od strane kompanije Microsoft. Tokom 2002. i 2003. godine je imao 95% korisnika u odnosu na druge brauzere dok se poslednjih godina usled pojave drugih, po mnogima boljih i naprednijih brauzera, procenat spustio na 55. Njegov osnovni pokretač je Trident. Trenutna verzija programa je u beta fazi i pod rednim je brojem 9 – Internet Explorer 9. Razvija se samo za Microsoft Windows.

7.2 Napadi , prevencije i alati

Kao najzastupljeniji brauzer, IE ima potencijalno najviše vrsta zlonamernog softvera od svih ostalih. Nažalost do sada najviše korišćena verzija 6, imala je jako slabu odbranu od napada štetnog softvera. Tek od verzije 7 počelo je sa alatima protiv zlonamernog softvera, a verzijom 8 se ozbiljno sa pravim rezultatima počeo pristupati problemu.

7.2.1 Napadi

Istraživači za Internet bezbednost kompanije Symantec dok su nadgledali spam napade od strane hakera, objavili su da su otkrili ranjivost ovog brauzera. Konkretni spam je imao naslovnu stranu vezanu rezervacije hotela gde su korisnici preko svoje elektronske pošte pozivani da rezervišu sobu sa linkom (vezom) ka oficijelnoj, ali kompromitovanoj stranici. Ta stranica je imala skriptu koja je proveravala koja se verzija brauzera i koji operativni sistem koristi. Skripta je aktivirana samo u slučaju korišćenja verzije 6 i 7 brauzera. Bez svog znanja korisnici su snimili zlonamernan softver i omogućili napadaču da pokrene bilo koji daljinski program (remote program) bez znanja korisnika. Taj zlonamernan softver se zvao backdoor Trojan dubbed Pirpi i startovao se zajedno sa servisom Netware Workstation. Dalje je kontaktirao određeni server, lociran u Poljskoj, u potrazi sa malim fajlovima sa .gif ekstenzijom koji su inače bili enkriptovani fajlovi sa komandama šta će dalje trojanac da radi. Microsoft je se svojim alatom Data Execution Prevention (DEP) u verziji 8 brauzera ispravio grešku i smanjio mogućnost ponovnih napada od istog trojanca.

U oktobru 2010. pojavilo se interesantno parče zlonamernog softvera. U pitanju je odlična imitacija Microsoft-ovog sigurnosnog paketa programa “Microsoft Security Essentials(MSE)“. Slike sa Malware Protection Cener sajta su pokazale da je ovaj štetan softver deprimirajuće dobar – odlično imitira MSE i svoj zadatak, ukoliko brauzer nije dobro zaštićen, obavlja prilično uspešno. Iskusniji korisnici ovog Microsoft-ovog paketa i računara uopšte neće biti prevareni, ali zato kod novih korisnika neće izazvati sumnju. Napad se vrši preko inficirane stranice koju je korisnik posetio i aktiviranja izvršnog fajla štetnog softvera - preko Drive-by-download-a. Prvo što radi, to je da se ubacuje u Windows-ov registar, a onda gasi veliki broj pokrenutih procesa u operativnom sistemu. Na kraju, prilikom pokretanja određenih programa koje “ne voli”, izbacuje MSE-olike iskačuće prozore koji obaveštavaju korisnika da je računar inficiran. Osim takvih

prozora, on pokušava preko linkova da natera korisnika da kupi nekoliko vrsta lažnih antivirusnih paketa.

7.2.2 Prevencije i alati

Prvi pravi pomak Microsoft-a u pravcu istinskog poboljšanja sigurnosti i zaštite od štetnog softvera je stvaranje nekoliko alata. U verziji 7 prvi put je implementiran alat tj. filter za zaštitu od pecanja korisnika. Nije bio aktiviran po klasičnim podešavanjima tako da je naknadno morao da bude uključen od strane korisnika. Filter proverava sajtove koje korisnik posećuje sa sigurnom listom koja se nalazi na microsoftovom serveru. Ako se poklapaju stranice nastavljaju slobodno da se učitavaju, ako ne onda brauzer izbacuje upozorenje za korisnika.

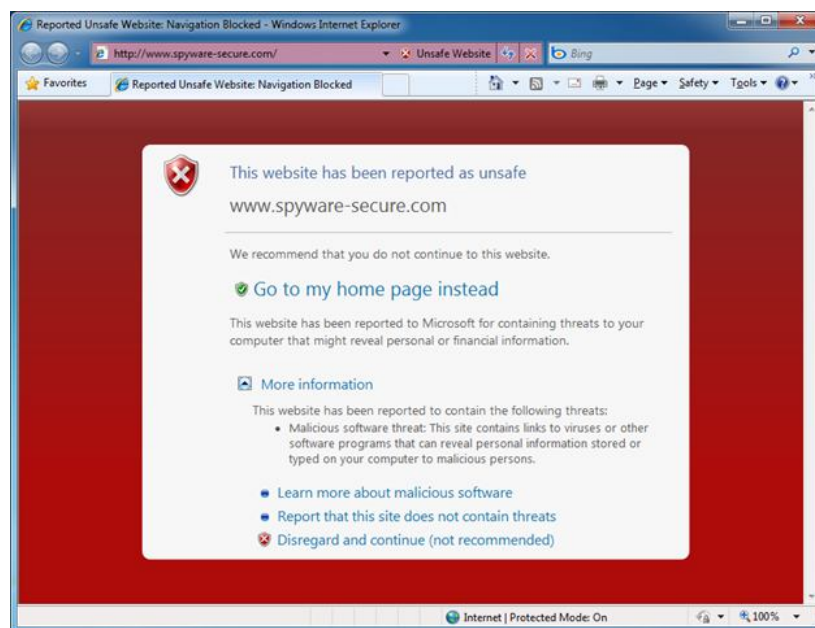
Microsoft je naglasio da se prilikom ove provere ne uzimaju lični podaci korisnika.

Za verziju 8 je razvijana unapređena verzija ove vrste filtera i naziva se SmartScreen Filter i koja radi na sličan način kao i prethodna verzija. Unapređenja su sledeća:

- **Poboljšan korisnički interfejs**

Korisniku koji prvi put uključuje Explorer pojavljuje se pitanje da li želi da SmartScreen bude uključen ili ne. Korisnik kasnije može to u opcijama programa da promeni.

Novi izgled upozorenja koje pojavljuje u slučaju učitavanja inficirane stranice na kome se



Slika 1.3 - Korisnički intefrejs SmartScreen filtera

nalaze link ka osnovnoj stranici(home page), crveno označena opcija nastavljanja ka toj stranici i informacije uopšte o zlonamernom softveru i savetima kako da se izbegnu opasne stranice.

- **Poboljšane performanse**

Pri radu osetno je manje usporenje brauzera nego pri ranijoj verziji.

- **Telemetrija i heuristika**

Razvijen je URL Reputation Service, servis koji vrši beleške o svim sajtovima koji sadrže opasan softver i pecanje za korisnike. U slučajevima pojavljivanja novih potencijalno opasnih sajtova, tj sajtova koji se sumnjivo ponašaju pri učitavanju, korisnik će biti upitan da li želi da prijavi taj sajt kao opasan ili kao bezbedan.

- **Podrška za grupne polise**

- **Privatnost**

Pri prikupljanju potencijalno opasnih sajtova, servis ne čuva te podatke zajedno sa IP adresom i drugim identifikujucim informacijama korisnika i sve informacije su enkriptovane.

Za verziju 9 brauzera koji je trenutno u beta fazi je došlo do još jednog ključnog unapređenja. Upravljač preuzimanja (download manager) je integrisan direktno sa SmartScreen filterom, stoga SmartScreen filter ima opciju snimanja reputacije sajtova, pomoću koje filter uklanja nepotrebna upozorenja od već dobro poznatih bezopasnih fajlova i prikazuje upozorenja kada su u pitanju fajlovi većeg rizika.

8. Google Chrome

8.1 Ukratko

Chrome je počeo da se razvija septembra 2008. godine od strane kompanije Google koristeći WebKit pokretač. Njegov osnovni kod je Chromium iz kojeg preko BSD licence koja omogućava da se program pravi kao otvorena (open source) ili zatvorena (close source) aplikacija. Po korišćenju je treći brauzer sa oko 8% procenata udela. Trenutna verzija je 7.0.517.41. Razvija se za Microsoft Windows, GNU/Linux i MAC OSX.

8.2 Napadi , prevencije i alati

Iako je mlad, ovaj brauzer ima već prilično razvijene alate protiv zlonamernog softvera. To i nije mnogo čudno, jer je stvoren od strane Google, kompanije za pretraživanje Interneta. Ta kompanija takođe preko svoje organizacije StopBadware.org identifikuje potencijalno inficirane stranice, a i mnoga rešenja već postoje u ovoj oblasti zahvaljujući drugim, starijim brauzerima.

8.2.1 Napadi

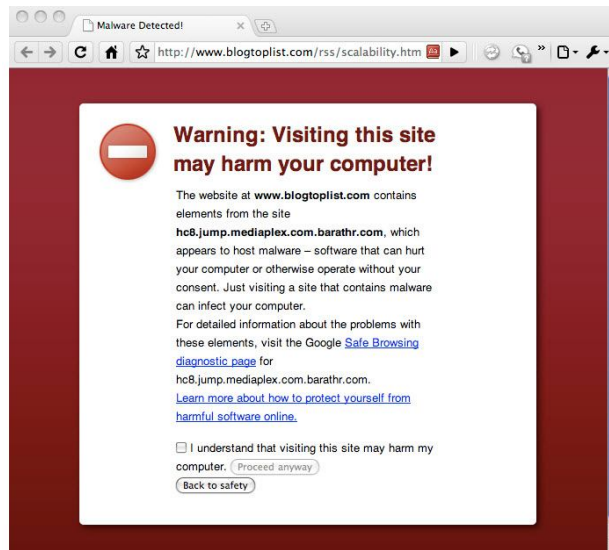
Napadači u poslednje sve češće stvaraju opasne programe upravo za Chrome. Jedan od takvih je cirkulisanje jedne nepoželjne elektronske pošte koja je tražila od korisnika ovog brauzera da instaliraju lažnu dodatak (ekstenziju). Kada korisnik klikne na link koji se nalazi u mail-u, instalira se zlonameran softver na računar. Antivirusna kompanija BitDefender je objavila da lažni Chrome dodatak izgleda isto kao pravi osim nekoliko znakova i ekstenzijom .exe na kraju, gde je originalni dodatak ima ekstenziju .crx. Posledica aktiviranja ovog štetnog softvera je promena Windowsovog HOST fajla koji posle blokira pristup sjatovima Google i Yahoo. Svaki put kada korisnik pokuša da im pristupi biva redirektovan na sajt vlasnika ovog zlonamernog softvera.

8.2.2 Prevencije i alati

Uprkos tome, čestim osvežavanjem programa i poboljšavanjem alata za sprečavanje širenja zlonamernog softvera, Chrome se vrlo dobro nosi sa ovim problemom. Kao što je prethodno navedeno jedna od grupa za delovanje protiv zlonamernog softvera je StopBadware.org, stvorena od kompanije Google koja i razvija Chrome. Chrome se takođe, kao i Firefox oslanja na crnu listu napravljenu i konstantno osvežavanu od strane StopBadware.org organizacije. Lista se stvara tako što Google pretražuje Internet i pronalazi nove i promenjene stare stranice.

Ove stranice se pronalaze preko linkova sa još takvih stranica, linkova stavljenih od strane vebmastera itd. Kad se primeti sajt koji izgleda kao potencijalni sajt za pecanje korisnika, on se dodaje listi osumnjičenih sajtova za pecanje, a kad se primeti sajt koji izgleda kao potencijalni izvor raznih vrsta zlonamernog softvera, startuje se virtuelna mašina koja istražuje taj sajt. Ako se detektuju na primer dodavanje virusa na stranicu, ta stranica se dodaje listi inficiranih sajtova zlonamernim softverom.

Pet minuta nakon starta programa, Chrome kontaktira Google servere i nakon toga svakih pola sata snima osvežene crne liste sajtova koji sadrže štetan softver i koji služe za pecanje



Slika 1.4 - Upozorenje za korisnika pri pristupu potencijalno inficiranog sajta

korisnika. Ove liste se čuvaju na računaru korisnika tako da se brzina rada brauzera i konekcije korisnika ne ugrožava, bar ne u velikoj meri.

9. Istorijat zlonamernog softvera

Jedan od prvih zlonamernih programa uopšte bio je virus Brain, nastao 1986. godine, od strane braće Farooq Alvi. Pri ulazu u računar (IBM PC), virus je inficirao boot sektore flopi diskova, koji su bili tada jedini fizički medij za transfer podataka. Klasični boot sektori su bili zamenjeni kopijom virusa, a originalni fajlovi su bili prebačeni u drugi sektor i označeni kao loši. Dolazilo je do usporavanja flopi diska i oko 7 kb memorije je bilo nedostupno za tadašnji operativni sistem DOS.

Pokušaj da se pročitaju inficirani boot sektori je uzrokovao redirekciju na ostale netaknute fajlove. Ovo je najranijija tehnika sakrivanja činjenice da na flopiju postoji bilo kakav opasan program i preteča danas kompleksnijih tehnika zataškivanja.

Prvi virus koji je koristio enkripciju bio je Cascade virus, nastao krajem 1986. godine. Koristio je enkripcija/dekripcija rutinu znanu kao decryptor – tehniku koja je kasnije usvojena kao deo skoro svakog zlonamernog softvera sa enkripcijom. Sa enkriptovanim virusima tadašnji antivirusi su imali velikih problema.

Prva značajna mutacija virusa desila se u julu 1995. godine, i nazivali su se makro virusi. Za razliku od boot sektor virusa, ovi su bili pisani u čitljivom formatu i ta činjenica kombinovana sa velikim brojem knjiga o makro programiranju dovela je do povećavanja broja novih makro i varijanti postojećih vrsta virusa. Tada su već računari bili povezani preko lokalne mreže (LAN) i to je dodatno uvećalo distribuciju virusa.

Sledeća velika promena načina funkcionisanja i stvaranja virusa bila je 1999. godine kada su se makro virusi počeli distribuirati preko email-a. Nastao je prvi zloglasni globalni virus, Melissa. Rezultat je bio razarajući virus, Love Letter, koji se proširio preko mejlova širom sveta.

Naredna velika promena desila se stvaranjem virusa koji su mogli da izvrše metamorfozu.

Win95/Regswap virus, nastao 1998. godine, je imao sposobnost da se prikrije na različite načine. Menjao je klasične x86 instrukcije i reprogramirao sam sebe.

2000. godine pojavio se ILOVEYOU, najskuplji računarski crv do tada koji je nanio štetu od 5,5 do 10 milijardi dolara. Širio se preko mejlova kao zakačen fajl. Još jedna važna promena dogodila se pojavljivanjem Open-World računarskog crva 2008. Imao je do tada nevidjenu mogućnost da komunicira sa svetom oko sebe (snimanje plugin-ova sa Interneta itd.) Upadom na računar povezivao ih je u svoj virtuelni računar kojim se moglo upravljati sa udaljenog mesta.

10. Vrste zlonamernog softvera

- 1. Virusi**
- 2. Trojanci**
- 3. Crvi**
- 4. Crimeware**
- 5. Scareware**
- 6. Rootkits**
- 7. Ransomware**
- 8. Backdoors**
- 9. Ransomware**
- 10. Potencijalno nepoželjni softver**

10.1 Virusi

Najvažnija specifičnost ove vrste zlonamernog softvera je da sam sebe može kopirati i tako zaraziti računar. Naziva se i parazitskim programom zato što se kači na fajlove ili but (boot) sektore i na taj način se širi prouzrokujući obilježan pad performansi operativnog sistema. Može se širiti preko lokalne mreže ili Interneta, preko flopi diska, CD-a, DVD-a, Blu-Ray-a, ili USB drajva.

10.2 Trojanci

Trojanski konj ili trojanac je vrsta opasnog softvera koja je zamaskirana kao nešto što je poželjno za instalirati i stoga korisnici vrlo često instaliraju ne znajući šta rade. U njemu se nalazi *payload* – opasan kod koji kao jednu od namena ima uništavanje određenih fajlova ili dalje instaliranje zlonamernog i nepoželjnog softvera. Hacker može da zameni neku dinamički povezanu biblioteku DLL sa trojancem koji će da obavlja isto ono što je i sama biblioteka i još nešto. To nešto može biti formatiranje particije čvrstog diska, krađa brojeva kreditnih kartica itd.

10.3 Računarski Crv

Računarski crv je vrsta štetnog softvera koji ima sposobnost da sam sebe reprodukuje koristeći mrežu i šalje svoje kopije na druge računare i najčešće bez znanja korisnika. Za razliku od virusa, crv ne mora da se zakači za postojeći program i šteta koju može da napravi je na primer, usporavanje konekcije.

Crvi imaju tri glavna dela:

1. Mehanizam napada

Mehanizam napada iskorišćava ranjivost operativnog sistema da bi se proširio na taj sistem.

2. Payload

Payload ne mora uvek da bude deo crva. Kad to nije slučaj, crv se samo širi i usporava ceo sistem, ali kad je payload sastavni deo crva može doći do preuzimanja administratorskih privilegija na sistemu ili instaliranja novih neželjenih programa

3. Izbor novih meta

Crvi imaju sposobnost da pronalaze nove mete sa već preuzetog računara. Code Red je računarski crv koji je zloupotrebljavao ranjivost Microsoft-ovog IIS (Internet Information Server) veb servera. Prva verzija Code Red crva je slala svoj opasni kod preko HTTP-a (Hypertext Transfer Protocol) raznim IP adresama. Da bi ovo uspelo bili je potrebno da se ispune sledeći kriterijumi:

- Postoji računar na poslatoj IP adresi
- Računar na toj IP adresi mora da ima uključen IIS
- Taj server ne sme biti zakrpljen ili zaštićen od tog crva

10.4 Crimeware

Crimeware je vrsta štetnog softvera napravljen (kroz socijalni inženjering) da izvrši krađu identiteta korisnika tj. da pristupi bankovnim i drugim računima i neovlašćeno prebaci novac na druge račune. Crimeware, takođe ima ulogu da iz mreže iznese, pokaže poverljive ili osetljive informacije radi finansijske eksploatacije.

10.5 Scareware

Predstavlja nekoliko klasa softvera za prevaru koji sadrži zlonamerne payload-ove koji se prodaju potrošačima koristeći određene vrste neetičkog marketinga. Korisnik se lažno obaveštava da na njegovom računaru postoji virus, stoga Internet kriminalci dalje predlažu da se snimi i plati (lažni) antivirus koji će ga obriše. Obično virus uopšte ne postoji, a antivirusni softver nije funkcionalan ili je ustvari zlonameran softver.

10.6 Rootkits

Rootkits predstavljaju razne vrste tehnika koje služe da sakriju zlonameran softver od detekcije ili dezinfekcije. Modifikuje se zaraženi operativni sistem da ne bi došlo do obaveštenja korisnika da se na računaru nalazi nešto što ne bi trebalo. Svaki operativni sistem pravi listu procesa koji se trenutno izvršavaju i rootkits tehnike sakrivaju zlonamerne procese koje se trenutno odvijaju.

10.7 Backdoors

Kada napadač već upadne na server koristeći različite tehnike, požeće da instalira backdoor. To parče softvera omogućava napadaču da sa udaljenog računara kasnije pokuša da kontroliše računar koji je zaražen. Na primer ako se sigurnosna rupa, koju je napadač prvobitno iskoristio da bi ušao u sistem, zatvori, instaliranjem backdoor-a neće morati da ponovi napad i tehnike koje su mu omogućile da prvi put upadne.

10.8 Ransomware

Ovaj zlonameran se najčešće pojavljuje u obliku crva, ulazi u sistem preko ranjivog mrežnog servisa ili kao fajl zakačen na email i može da isključi važne servise za operativnog sistema ili da zaključa važne fajlove korisnika. Razlika u odnosu na prethodne programe, zahteva otkup da bi se sistem vratio u prvobitno stan

10.9 Potencijalno nepoželjni softver

10.9.1 Spyware

Ovo je tip zlonamernog programa koji kad se instalira na računar sakuplja informacije o korisniku bez njegovog znanja. To su informacije o sajtovima koje korisnik najčešće posećuje, koje programe ima instalirane, koji je antivirus aktivan itd. Mogućnosti spyware-a nisu samo jednostavno praćenje korisnika nego i preuzimanje kontrole nad sistemom, kao što je instaliranje dodatnih programa, upućivanje na druge Internet sajtove preko brauzera, menjanje podešavanja internet konekcije gde dolazi do uspostavljanja i/ili diskonekcije.

10.9.2 Zlonamerni adware

Adware je softver koji ima ulogu da automatski prezentuje, prikazuje i snima reklame koje mogu doći u obliku iskaćućeg prozora. na računaru. U najvećem broju to su legitimni softverski paketi, ali u nekim slučajevima na primer, BonziBuddy, aplikacija označena kao inteligentni softverski agent, inficira mnoge sistemske fajlove i prikazuje nelegalne reklame.

10.9.3 Dialer

Parče koda koji prebacuje uglavnom dial-up konekciju sa regularnog Internet davaoca usluga na neki drugi koji će korisniku preko telefonskog računa višestruko naplatiti.

10.9.4 Administratorski alat za daljinsko korišćenje

Kad se ovakav alat napravi od strane trećeg neovlašćenog lica, može biti velika bezbednosna pretnja.

10.9.5 Provaljivač lozinki

Mali program koji služi za vraćanje zaboravljenih lozinki korisnika ili administratora. Kad je u rukama napadača, najčešće dolazi do ugrožavanja privatnosti i sigurnosti.

10.9.6 Joke – šala

Softver koji u sebi nema zlonameran kod ili payload, ali upozorava na to tj. nervira korisnika.

11. Vrste napada na veb brauzere, strategije i tehnike odbrane

Najčešći oblici napada kroz brauzer i elektronsku poštu su:

1. Socijalna manipulacija - Phishing
2. Drive-by download

11.1 Socijalna manipulacija

Ovaj termin opisuje ne-tehničku vrstu upada u računar korisnika, tačnije oslanja se na interakciju između ljudi i često se pokušava prevariti korisnika da bi se došlo do osjetljivih informacija. Napadač pokušava da stekne poverenje nekoga ko ima regularan pristup nekoj mreži, recimo banci, i da ga navede da otkrije poverljive podatke.

Drugi aspekt socijalne manipulacije se oslanja na čestu osobinu korisnika, a to je da nije svestan kolika je vrednost određene informacije koju poseduje i stoga neobazrivost po pitanju zaštite takve informacije.

11.1.1 Phishing – pecanje

Pecanje predstavlja zlonameran pokušaj preuzimanja osjetljivih informacija od korisnika kao što su bankovni računi, medicinski podaci, šifre i korisnička imena posećenih sajtova socijalnih mreža, foruma, preko zamaskiranja i stvaranja lažnih sajtova, mejlova itd. Falsifikuju se veb sajtovi na kome korisnik ostavlja broj kreditne kartice radi provere bankovnog računa ili ostale lične informacije (socijalne mreže), šalju se mejlovi sa obaveštenjem da korisnik osveži svoje podatke i linkom ka falsifikovanoj stranici. Ukratko, krađa, samo preko Interneta. U većem broju slučajeva pecanje se obavlja slanjem lažne elektronske pošte nazvane *spam*.

Nastalo je od reči engleske reči *fishing*, u prevodu ribolov, i žargonski prebačeno u phishing verovatno pod uticajem na reč *phreaking*, i aludira na mamac koji se upotrebljava za hvatanje važnih informacija od korisnika. Ova tehnika je prvi put opisana 1987. , a termin pecanje je nastao 1996. godine.

Pecanje je primer socijalne manipulacije da bi se korisnik prevario i gde se iskorišćava slaba upotrebljivost trenutnih bezbednosnih veb tehnologija. Ovo je najčešći oblik socijalne manipacije.

11.1.1.1 Napadi

Prvi slučajevi pecanja su vezani za AOL – America Online, veliki davaoc Internet usluga u SAD. Napadači su se predstavljali kao službenici te kompanije i slali instant poruke korisnicima, tražeći im da otkriju svoje šifre. Da bi naveli korisnike, kao razlog davanja šifre navodili su imperative kao što su “verifikacija naloga” ili “potvrđivanje informacije o naplati”. Kad dođu do šifre, napadači su pristupali daljem slanju neželjene pošte ka kontaktima korisnika.

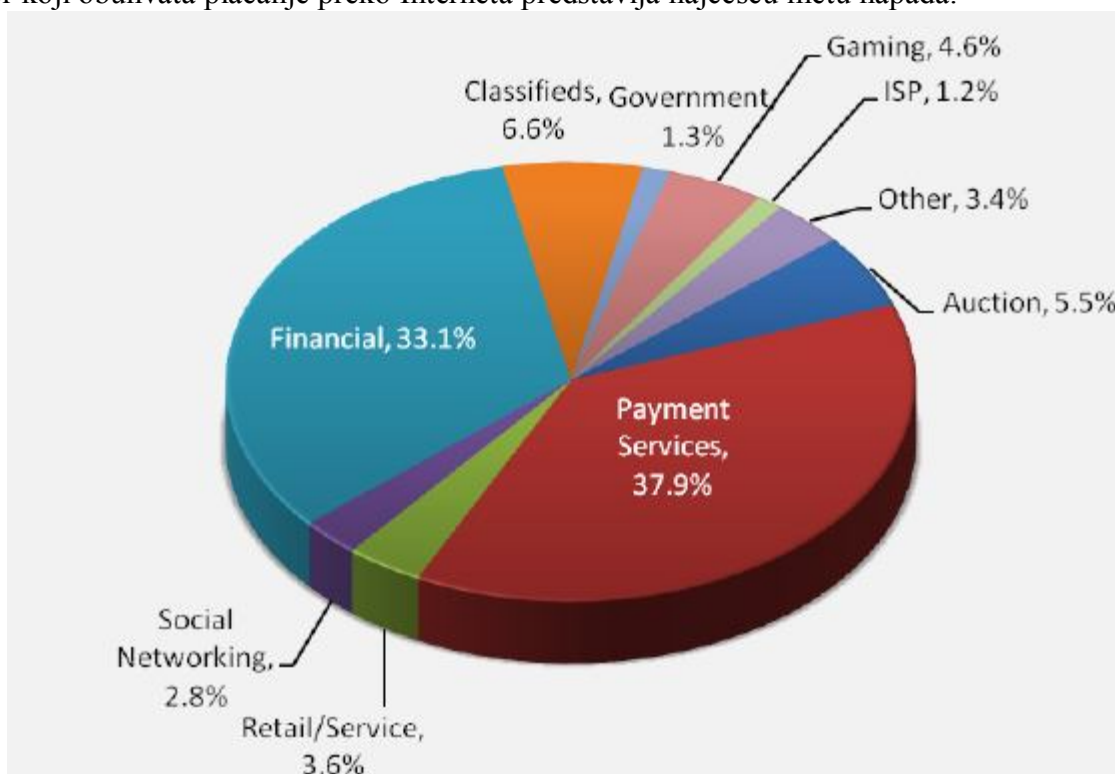
Napadači koriste ovu tehniku i za slanje email-a sa navodno IRS-a (američke poreske službe) i krali osetljive podatke poreskih obveznika.

Prvi primeri napada na korisnike banaka koji pristupaju svojim računima preko Interneta su bili nasumični. Poslednja istraživanja pokazuju da napadači koriste kao metu na primer izvršne direktore banaka i drugih institucija i druge ljude visokih profila poslovanja.

Poslednjih godina, pojavljivanjem i razvojem sajtova za socijalno umrežavanje kao što su Facebook ili MySpace, mete pecanja su korisnici ovih sajtova. Cilj je krađa identiteta tj. naloga. Eksperimenti pokazuju da je uspešnost napada na socijalne mreže oko 70%.

Sajt za deljenje velikih količina fajlova, kao što je Rapidshare je označen kao meta za krađu premijum korisničkih naloga, naloga koji se inače naplaćuju.

APWG je globalna organizacija za sprečavanje širenja pecanja, krađe identiteta i drugih oblika perversa na Internetu. Prema poslednjem izveštaju ove organizacije za drugi kvartal 2010. godine sketor koji obuhvata plaćanje preko Interneta predstavlja najčešću metu napada:



Grafikon 1.1 – Najčešće mete napada

Prema istom izveštaju država sa najvećim procentom Internet stranica sa tehnikom pecanja su SAD:

April		May		June	
USA	74.88%	USA	84.12%	USA	68.17%
China	2.97%	UK	1.57%	Canada	3.94%
UK	2.29%	Germany	1.50%	UK	3.40%
Rep. Korea	2.05%	Canada	1.21%	Germany	3.15%
Germany	2.01%	France	1.16%	France	3.04%
France	1.67%	China	1.03%	China	1.98%
Netherlands	1.58%	Brazil	0.83%	Rep. Korea	1.53%
Canada	1.57%	Australia	0.74%	Netherlands	1.44%
Hong Kong	0.90%	Netherlands	0.72%	Brazil	1.39%
Italy	0.76%	Rep. Korea	0.66%	Hong Kong	1.09%

Grafikon 1.2 – Procenat Internet stranica sa tehnikom pecanja

11.1.1.2 Izmena linka

Napadač slanjem neželjene pošte (*spam*) koja ima naslov neke lažne kompanije ili banke koja je sličnog naziva kao regularna banka korisnika. U mejlu se nalazi najčešće link regularne banke, ali sa malom greskom koju korisnik često ne primeti i koji vodi ka prevarantskom sajtu.

Drugi metod je ubacivanje @ znaka u link: <http://www.google.com@members.tripod.com/>

Ovo može navesti korisnika da ce da se otvori stranica na www.google.com , a ustvari će prebaciti brauzer na members.tripod.com.

Kao što je pomenuto u prvo delu, prilikom izrade ovog rada i prilikom pokušaja otvaranja linka: <https://wwwse.inf.tu-dresden.de/wiki/images/f/f6/PRO-TimLackorzynski.pdf> došlo je do upozorenja brauzera da je to moguća inficirana stranica. Ovo je klasičan primer mogućeg zlonamernog iskorišćavanja tehnike URL (Uniform Resource Lokator) redirektovanja, gde se korisnik može prebaciti na stranicu sa koje se može neželjeno snimiti neki zlonameran program ili lažni antivirusni program.

11.1.1.3 Falsifikovanje sajtova

Neke tehnike napada upotrebljavaju JavaScript komande da bi na primer stavili sliku legitimne adrese sajta preko adresnog dela veb brauzera. Kada korisnik slučajno upadne na lažan sajt, prava adresa se na taj način maskira. *Cross Site Scripting* je vrsta napada koja koristi mane skipte veb stranice gde se korisnik upućuje na deo stranice koja služi za upis korisničkog imena i šifre. Ova

tehnika je posebno problematična, jer i veb adresa sajta i sigurnosni sertifikati izgledaju onako kako bi trebalo, otežavajući običnim korisnicima da to primete.

11.1.2 Anti-phishing – anti-pecanje

Postoje tri različita pristupa koje sadrže mnoštvo specifičnih tehnika koje efikasno, u manjoj ili većoj meri, štite obične korisnike Interneta od pecanja. Jedan je socijalni, drugi zakonodavni pristup, a treći se tiče tehnologije.

11.1.2.1 Socijalni pristup

Klasična metoda socijalnog pristupa je edukacija Internet korisnika. Preko reklama na sajtovima koji imaju veću posećenost, naučnih, ali prosečnim korisnicima jasnih, tekstova na blogovima i štampanim medijima itd prosečni korisnici mogu bolje shvatiti opasnosti koje postoje na Internetu. Kada primi email koji sadrži informacije o njegovom bankovnom ili nekom drugom računu i ako postoji neki link sa imenom oficijalne stranice, korisnik bi trebalo da proveri da li je to pravi email u pitanju. Korisnici takođe ne bi trebalo da klikću na svaku drugu reklamu koju vide i koja obično nudi neke besplatne usluge ili brzu zaradu, jer postoji velika mogućnost da će završiti na stranicu stvorenu od napadača.

Neke kompanije kao na primer PayPal, obraćaju se svojim korisnicima preko elektronske pošte njihovim korisničkim imenom. Ako email počinje sa „Dragi PayPal korisniče” najverovatnije je u pitanju *spam*. Elektronska pošta od strane banaka često sadrži delove broja kreditne kartice korisnika. Međutim, skorija istraživanja pokazuju da prosečan korisnik ne pamti razliku između početnih i poslednjih brojeva kartice, a to je problem, jer svi korisnici iste banke imaju obično iste početne brojeve. Napadači to mogu da iskoriste tako što će u svom mejlu (*spam-u*) staviti nasumične brojeve i prevariti korisnika. Pokušaji pecanja tokom 2006. godine pokazala su da lične informacije koje kompanije stavljaju u svoju oficijalnu elektronsku poštu, ne smanjuju broj uspeših pecanja. Prosečni korisnici ne obraćaju puno pažnje na takve detalje.

11.1.2.2 Zakonodavni pristup

Od 2004. godine, pa nadalje bilo je nekoliko hapšenja i presuda licima koji su se bavili ovom vrstom prevare. 26. januara 2004. Federalna Trgovinska komisija SAD-a je podnela tužbu protiv osobe osumnjičene za pecanje. Kalifornijski adolescent je napravio lažnu Internet stranicu koja je izgledala isto kao sajt AOL-a (America Online) i koristio je da krade novac sa kreditnih kartica. 2006. god. osam ljudi je uhapšeno od strane japanske policije pod sumnjom da su napravili lažne Yahoo stranice i ukrali oko 870.000 američkih dolara.

Da je američki kongres usvojio predlog zakona *Anti-Phishing Act of 2005*, svaki kriminalac koji se bavio ovim aktivnostima bio bi osuđen na kaznu do 250.000 dolara i zatvorsku kaznu do 5

godina. Trenutno je na snazi *Anti-Phishing Act of 2006*. u nekoliko država SAD-a. Britanci su *Fraud Act 2006* usvojili i doprineli da osuđeno lice može dobiti zatvorsku kaznu do 10 godina.

I kompanije su se uključile da bi zaustavili pecanje. Microsoft je okružnom sudu u Vošingtonu predao 117 optužnica protiv nepoznatih lica zbog krađe šifara i poverljivih informacija, a tokom 2006. godine predao 100 optužnica izvan SAD-a. Davaoc Internet usluga Earthlink je pomogao pri identifikovanju 6 osoba osumnjičenih za prevaru tehnikom pecanja u Konektikatu.

Za svaku vrstu Internet kriminala zakoni se teško donose i još teže primenjuju. Tehnologije i tehnike kako pecanja tako i pravljenja virusa, računarskih crva i ostalih zlonamernih programa se konstantno menjaju i usavršavaju. Da bi došlo uopšte do nekakve optužnice, a posle i presude, zakon mora da obuhvata sve trenutne tehnologije zaštite od pecanja, tehnike samih napadača i sve pojmove koji su za to vezani.

11.1.2.3 Tehnološki pristup

Postoji nekoliko različitih tehnika za sprečavanje ili bar umanjivanja šansi da neko treće lice tj. napadač ilegalno dođe do važnih podataka. Ovo su neke od efikasnijih tehnika:

- *Trusted path*

Ova se tehnika uglavnom koristi pri razmeni podataka između korisnika i neke finansijske institucije, recimo banke. Za komunikaciju brauzera sa sajtovima koji imaju obavezu da zaštite podatke koriste se digitalni sertifikati. Kad se korisnik povezuje sa bankom preko svog brauzera dobija sertifikat od same banke koji jeste zaštićen, ali napadač može doći u posed takvog sertifikata i ukrasti podatke. *Trusted path* je tehnika koja koristi javni ključ gde korisnik enkriptuje svoje podatke pre slanja. Međutim, ako pokuša da ih dekriptuje, napadač neće uspeti, jer dekriptovanje tj. otvaranje tih podataka zahteva privatni ključ koji poseduje samo banka. Tako zaštićeni podaci ne mogu doći u pogrešne ruke.

- Hashing passwords

Korisnici jako često koriste iste šifre za više sajtova, jer im je lakše da zapamte. Ako napadač uspe da uhvati jednu šifru velike su šanse da to zloupotrebi na više strana i napravi veću štetu. Tehnika se sastoji u tome da recimo banka doda samoj šifri određeni specifični domen koji koristi i onda takva šifra postaje sigurno autentična.

- Dvostrana autentifikacija

Zasniva se na čestom menjanju šifara korisnika ili korišćenju specijalnog modema koji će da obavlja enkripcije podataka koji se šalju. Ovu tehniku najčešće koriste banke i druge velike finansijske institucije.

- Analiza novčanih transakcija

Ako je neki novac prebačen iz banke, tj. sa određene IP adrese na neku nepoznatu IP adresu sajta koji korisnik nikad pre nije ni posetio, tad se može znati da je najverovatnije izvršena krađa. Ovakvim analizama se pre mogu baviti kompanije nego sami korisnici.

- Anti-phishing toolbars

To su dodaci tj. alati koji se nakon instalacije pokreću zajedno sa brauzerom. Ako se tehnika napadača sastoji u maskiranju URL adrese, alati imaju mogućnost da korisnika na to upozore.

11.2 Drive-by download

Napadi preko preko drive-by download-a su među najrasprostranjenijim metodama koje se koriste za ubacivanje zlonamernog softvera u računarske sisteme. Ovakvi napadi se vrše isključivo preko veb brauzera pristupanjem inficiranoj stranici gde se zloupotrebljava ranjivost memorije brauzera i njegovih plug-in-ova radi izvršavanja *shellcode-a (payload-a)*. Snimanje zlonamernih programa na ovaj način se dešava bez znanja korisnika kao i kod svih ostalih metoda i dolazi do krađe šifara i korisničkih imena korisnika, drugih važnih i osetljivih podataka, brisanje podataka itd.

Klasični koraci pri drive-by download napadu:

1. Napadač priprema legitimnu Internet stranicu da bi ubacio svoj zlonameran kod. Vrlo često se koriste plugin-ovi ili ekstenzije popularnih veb brauzera, jer se takvi dodaci prave od trećih lica tj. od programera nezavisnih od kompanija koje prave same brauzere. Kao takvi manje su testirani od brauzera i stoga najverovatnije imaju više sigurnosnih rupa. Zlonameran kod dolazi preko dodataka u brauzera, a preko brauzera u operativni sistem.
2. JavaScript je jedna vrsta skriptovanog koda koja se koristi kod nekih brauzera i najčešće se koristi da bi se *shellcode* aktivirao preko tehnike koja se zove heap spraying. Ova tehnika omogućava opasnom kodu da se proširi memorijom i kontroliše neke njene delove. Kada napadač na ovaj način spremi opasni kod, ubacuje ga na legitimnu stranicu.
3. Da bi se običan korisnik privukao da poseti baš tu stranicu, napadači pribegavaju raznim tehnikama. Mogu napraviti novu stranicu (sa redirekcijom na legitimnu inficiranu stranicu), pa manipulisanjem pretraživača (Google, Yahoo) postaviti je na vrhu liste nađenih stranica ili mogu na popularnim veb sajtovima postaviti reklame koje će korisnika ukoliko na njih klikne odvesti do inficirane stranice. Kada korisnik dođe do ove stranice, zlonameran JavaScript kod ulazi u brauzer i aktivira se.
4. Napadač kontroliše korisnika – žrtvu.

11.2.1 Implementacija tehnike za otkrivanje napada preko drive-by download metode

IT stručnjaci i inženjeri Secure Systems Lab-a uz pomoć Austrijske naučne fondacije stvorili su prototip tehnike za otkrivanje širenja zlonamernog programa preko metode drive-by download, metode koja isključivo funkcioniše kroz veb brauzer.

Ovu tehniku istraživači su primenili samo na brauzer Mozilla Firefox, jer je osnovni kod od kojeg je napravljen otvorenog tipa i svako ga može pod određenim uslovima koristiti.

Svaki brauzer ima svoj način primene ECMA-262 standarda koji definiše osnove objektnog jezika za skriptovanje u brauzeru i nekim drugim aplikacijama. Firefox koristi JavaScript jezik preko interpretatora koji se naziva SpiderMonkey i cela implementacija je primenjena koristeći uslove koje ovi standardi definišu.

Tokom eksperimenta posećena je stranica www.thewebleaders.com koja je u sebi imala *inline frame (iframe)* deo koda koji se dodaje unutar stranice da bi došlo do učitavanja druge stranice (inficirane), obično sa drugog servera. Kao što je rečeno, drive-by download metoda se sastoji u napadu na ranjivu memoriju brauzera pre nego uspešno aktivira zlonamerni program. To se čini koristeći skriptu koju brauzer koristi. Tehnika otkrivanja opasnog koda je u tome da neprestano prati sve stringove koje dodeljuje SpiderMonkey tražeći *shellcode*, tačnije opasan kod i kada ga sistem pronade izvršavanje skripte se zaustavlja.

11.2.1.1 Efikasnost tehnike

Lista URL-ova, sakupljene preko neželjene pošte jedne srednje kompanije i Spamcop veb servisa, činila je ukupno 11,910 URL-ova sa 1,187 tragova sa opasnim kodom. Svaka stranica je sačuvana na lokalni server odakle se vršila pretraga za opasnim kodom. Od tih 1,187 tragova, prototip ovog sistema je otkrio 956 primeraka *shellcode*-a, dakle 81% efikasnosti.

Kasnije je provereno zašto sistem nije prepoznao ostalih 231 primeraka.

Prva grupa (62 traga) su vrste zlonamernog softvera koji ne zloupotrebljavaju ranjivost memorije brauzera.

Druga grupa od četiri traga ne koristi JavaScript nego Visual Basic skriptu.

Kako je prethodno rečeno, otkrivanje zlonamernog koda nije vršeno sa direktno sa Interneta nego sa lokalnog servera, i stoga treća grupa (od 127 tragova) nije prepoznata zbog grešaka u JavaScript-u.

Četvrta grupa (38 tragova) su lažni.

11.2.1.2 Optimizacija performansi

Čitav proces utiče na performanse tj. brzinu učitavanja bilo kojih stranica od strane brauzera i neke strategije su primenjene da bi dolazilo do što manjeg usporavanja. Pri učitavanju, uvek se pojavljuju neki string objekti koji se moraju proveriti. Ali jedna od strategija se sastoji u tome da se snime sve informacije vezane za sve kreirane string objekte i kasnije da se izvrši pretraga za opasnim kodom. Nakon testa performansi koji je uključivao učitavanje 150 najpopularnijih sajtova (prema Alexa-i, kompaniji za istraživanje Interneta) i brzinu konekcije od 1Mbit/s koristeći prvo običnu verziju Firefox-a, nakon toga modifikovanu verziju koja sadrži ovaj sistem bez optimizacija performansi i na kraju modifikovanu verziju sa ovim sistemom sa optimizacijom performansi, pojavili su se sledeći rezultati:

		Ukupno vreme (s)	Vreme po stranici (s)
Regularni brauzer		527	3.51
Zaštićen brauzer	bez optimizacije	1,237	8.25
	sa optimizacijom	876	5.84

Grafikon 1.3 – Performanse brauzera pre i posle optimizacije

Prema ukupnom istraživanju i pronalasku svih opasnih kodova koji su imali tačno onu funkciju za koju je ovaj sistem i napravljen može se zaključiti da je ova tehnika gotovo stoprocentna i da nakon optimizacije performansi, brzina učitavanja stranica se približava onoj koja se postiže klasičnom, nezaštićenom verzijom brauzera.

12. Uloga organizovanog kriminala i finansijski aspekt

Prvih 15 godina zlonamerne programe kao što su virusi i poneki računarski crv i pravili su ih mladi entuzijasti da bi iz čistog hira naudili nekoj drugoj osobi, dok danas postoje više od deset vrsta štetnih programa uključujući spyware, crimeware, ransomware, rootkits, backdoors, trojance itd. Ovi se programi se danas u većini prave u dobro organizovanim kriminalnim grupama koje nanose veliku finansijsku štetu direktno ili indirektno legalnim kompanijama koje pružaju usluge od proizvođača regularnih programa, upravljača mreža, davaoca Internet usluga do samih korisnika. Troškovi mogu da uključe preventivne mere, troškove protoka podataka i opreme itd.

12.1 Botnet

Prevaranti i kriminalci najviše koriste botnet-e, servise za izdavanje sajtova sa slabom zaštitom i bave se manipulacijom cena akcija. Botneti su manje ili veće mreže računara na kojima se nalaze originalni zlonamerni programi odakle se šalju na Internet. Prema kompaniji za Internet bezbednost Marshal, 85% botnet spam-a dolazi od samo 6 botnet-a, gde su najveći Srizibi (39%) i Rustock (21%). Srizibi najčešće preko neželjene pošte šalju trojance i tu su najnapredniji. Istraživanje takođe pokazuje da ovaj botnet pruža povratne informacije i statistiku o tome koje su email adrese bile dobre, a koje nisu. Ostali botneti sa značajnim udelom u širenju zlonamernog softvera su Mega-D, Hacktool.Spammer, Pushdo i sa sve manjim uticajem, Storm.

12.2 Finansijski aspekt

Finansijski uticaj zlonamernog softvera ima dve strane. Sa jedne, kompanije koje pružaju bezbednosne usluge stvaraju nove poslovne aktivnosti i nova radna mesta kojih ne bi bilo da nije takvih programa. Sa druge strane, bankarske usluge i druge finansijske transakcije koje se obavljaju preko Interneta su često meta napada kriminalaca i povećavaju se troškovi povećanih mera bezbednosti i uklanjanja nanete štete što itekako utiče na korisnike.

Zlonamerni softver sa današnjim tehnikama upada u zaštićeni sistem i alatima koji imaju mogućnost da se bez naprednog poznavanja programiranja naprave gotovi štetni programi što predstavlja jeftini, ponovo upotrebljivi metod Internet kriminala.

Prema studiji International Telecommunication Union, sumirajući prikaz finansijskog aspekta zlonamernog softvera izgleda ovako:

- Otprilike 13,2 milijarde dolara u SAD (2006. godine) na globalnu ekonomiju i do 67,2 milijarde direktnog ili indirektnog efekta u poslovnoj sferi (2005. godine)
- Računarski Institut za bezbednost – Computer Security Institute (CSI) procenio je gubitak prouzrokovan sigurnosnim propustima od oko 345000 dolara.

- Časopis za izveštaje potrošača Consumer Reports, je objavio da su direktni troškovi potrošača, uzrokovani od strane zlonamernih programa i spam-a, na teritoriji SAD do 7,1 milijarde u 2007. godini
- Jedno predviđanje stavlja ukupne troškove zbog neželjene pošte od 100 milijarde dolara u 2007.
- Prema nekim izvorima, ukupna siva ekonomija vredi oko 105 milijardi dolara.

2009. godine, Nukleus Research je objavio da američke kompanije izgube zbog spam-a 712 dolara po zaposlenom godišnje. Izračunato je da svaki poslovni korisnik od 3 primljene elektronske pošte, primi dve koje su *spam*. Kao rezultat, poslovni korisnici provedu 16 sekundi identifikujući i brišući neželjenu poštu što dovodi do 70 milijardi gubitka za ceo poslovni svet.

13. Predviđanja širenja i razvitka zlonamernog softvera

WebSense je kompanija za istraživanje Internet bezbednosti. U izveštaju za 2010. godinu se navodi da je njihov alat za skeniranje pregledao svakog sata oko 40 miliona veb sajtova i približno 10 miliona mejlova. Rezultati su sledeći:

- 111.4 % je povećanje inficiranih Internet stranica u proteklih 10 godina.
- 79.9% koji su sadržali opasan kod su bili legitimni sajtovi koji su bili inficirani bez znanja vlasnika.
- 52 procenta krađa podataka je izvršena preko Interneta
- 89.9% neželjene elektronske pošte sadržalo je linkove ka sajtovima za pecanje i/ili sajtovima sa inficiranim stranicama.
- SAD i Kina nastavljaju da budu vodeće zemlje u količini zlonamernog softvera
- 23% sajtova koji se tiču zabave imali su opasan kod.
- 40 procenata svih Facebook statusa su imali neki link, a 10 posto njih su vodili ili ka sajtu za pecanje ili sa opasnim kodom.

Glavni razlog ovog trenda je u povećanju znanja i dostupnosti informacija u vezi samih programa ovakve namene. Programa koji su štetni kako po obične tako i po poslovne korisnike. Prema časopisu Hakin9 koji se godinama bavi ovom temom, postoji nekoliko predviđanja kakva će biti budućnost sajber kriminala.

1. Napadi na direktnu maloprodaju i maloprodaju preko Interneta će se povećavati u odnosu na napade na banke i druge finansijske institucije

Banke postaju sve pametnije. Shvataju da sajber kriminal pokušava da opljačka njih, jer se najveći novac upravo tu nalazi. FDIC – Federal Deposit Insurance Corporation u SAD-u daju obavezu bankama da uvedu sigurnosnu zaštitu svojih podataka. Ako ne ispoštuju, banke plaćaju kaznu od 1 milion dolara. Stoga bankama se više isplati da ulažu u nove tehnologije kao što su UTM zaštitni zidovi (firewalls), IPS uređaji sledeće generacije, Network Access Control (NAC) i Physical Access Control (PAC) rešenja.

Sa druge strane, prodavnice maloprodaje ne pokušavaju da dostignu nivo zaštite koju imaju banke iako su pod velikim pritiskom VISA, MasterCard i drugih kompanija kreditnih kartica. Maloprodajni objekti koriste bežični Internet za podršku njihovim fiskalnim kasama i bar kod skenerima – ovo često dovodi do sajber kriminalaca koji sede u svojim automobilima na parkiralištima preko laptopova upadaju u sisteme.

2. Računarstvo u oblacima (Cloud Computing) i virtuelne mašine

Istraživanja na Univerzitetu Kalifornija u San Dijegu i na Tehnološkom Institutu u Masačusetsu pokazala su ranjiva mesta u računarstvu u oblacima i virtuelnim mašinama.

3. Napadi na pametne telefone i PDA uređaje preko aplikacija

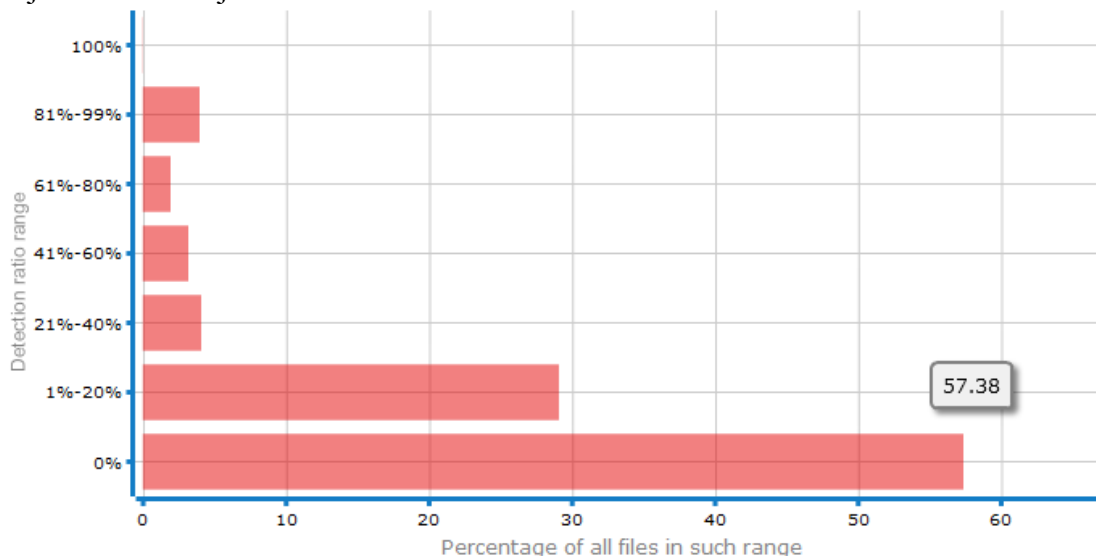
Geotagging je jedan od najvećih rizika za korisnike pametnih telefona. Kada korisnik šalje snimljenu fotografiju na primer na svoj Twitter nalog, on ponekad ne šalje samo tu fotografiju nego aplikacija koja se za to upotrebljava šalje informaciju zajedno sa slikom o tome gde se korisnik trenutno nalazi. Tako nešto korisnik ne vidi bez odgovarajućih programa ili dodataka za brauzer. Zbog toga što korisnici bezuslovno veruju besplatnim aplikacijama za njihove telefone, dovešće najverovatnije do povećanja zlonamernog softvera u ovim aplikacijama koji će moći da ukrade identitet korisnika, prisluškivanja razgovora itd.

4. Voice over Internet Protocol (VoIP) napadi će biti sve učestaliji

VoIP ostaje nesigurna platforma koja se lako može hakerisati. Prema National Vulnerability Database postoji skoro 100 najčešćih vrsta ranjivosti ovog načina komunikacije. Napadi će biti usmereni na presretanje poziva, krađe poruke koje idu preko glasovne pošte i sl.

5. Eksponencijalni rast inteligentnog zlonamernog softvera

VirusTotal je besplatan servis stvoren od kompanije Hispasec Sistemas koji ima ulogu da analizira sve potencijalne viruse, crve, trojance i druge vrste štetnog softvera koji su otkriveni ili nisu otkriveni d strane antivirusnih programa. Servis analizira oko hiljadu uzoraka štetnog softvera pomoću 40 alata i vidi se iz sledećeg grafikona da kućni antivirusi u više od polovine slučajeva ne otkrivaju zlonamernan softver:



Grafikon 1.4 – Skoro 60% neotkrivenih primeraka zlonamernog softvera

6. Kreativnija socijalna manipulacija

Socijalna manipulacija koja uključuje napadača koji se predstavlja kao administrator kompanije sa kojom posluje korisnik i koji od istog korisnika traži njegovu šifru, jer su se podaci navodno zagubili, su prošlost. Danas korisnik bez potrebnog znanja, bez dovoljnih informacija o inovativnim načinima socijalne manipulacije i bez potrebne opreme (noviji modemi, UTM uređaji itd.), biće gotovo sigurno izmanevrisan i prevaren.

7. Povećanje ranjivosti aplikativnog sloja u operativnom sistemu Windows

Jedna od skoro otkrivenih grešaka u programu za čitanje PDF fajlova, Adobe Acrobat Reader-u, je dovela do zloupotrebe od strane napadača. Kompanija Adobe nije jedina. Internet Explorer, kompanije Microsoft, je imao ranjivost pri otvaranju fotografija formata JPEG, ali je taj problem rešen. Pitanje je da li možda sad postoji slična greška kod formata PNG? Da li će neki haker napraviti parče koda koji će zloupotrebiti ovu grešku i preuzeti kontrolu nad nekim računarom preko brauzera i tehnike drive-by download tako što će brauzer kada učitava legitimnu (ali inficiranu) stranicu koja sadrži PNG fajl snimiti taj štetan program? Svakodnevne aplikacije kao što su Outlook Express, neki FTP program ili veb brauzer svojim novim verzijama dobijaju nove opcije koje mogu i sadržaće neke greške, tj. potencijalna mesta za zloupotrebu.

14. Uticaj zlonamernog softvera na Veb 2.0

Socijalne mreže zauzimaju sve veći Internet prostor, jer daju svima mogućnost da preko svojih profila prave drugačiju (bolju) sliku o sebi i da imaju što veći broj prijateljstava. Facebook je najveća takva mreža sa preko 500 miliona korisnika, druga je Twitter sa 190 miliona, a na trecem mestu je MySpace sa 37 miliona. Što više ljudi bude koristili ove mreže, biće više mogućnosti za širenje zlonamernog softvera i socijalnu manipulaciju korisnika od strane hakera i sajber kriminalaca.

14.1 Veb 2.0

Termin Veb 2.0 ne opisuje određenu tehnologiju nego evoluciju u razvoju Internet resursa vođenom i tehnološkim i društvenim silama. Raznovrsnost tehnologija kao što su AJAX - Asynchronous JavaScript and XML i RIA - Rich Internet Applications (Adobe Flash i Microsoft SilverLight) omogućavaju stvaranje interaktivnijih i vizuelno atraktivnijih aplikacija. Ovaj prelaz polako briše liniju razdvajanja između mogućnosti Internet i klasičnih desktop aplikacija.

Prethodna generacija veba takozvani Veb 1.0 je bio fokusiran na prebacivanje tradicionalnog poslovanja na Internet dok se Veb 2.0 fokusira na umrežavanje korisnika (Facebook, MySpace, Twitter) i ohrabrivanje korisnika da sami stvaraju sadržaj i postavljaju ga na Internet (YouTube i Flickr). Kompleksnost samih veb aplikacija se povećala i stoga omogućila nove načine napada od strane hakera.

Veb 2.0 sajtovi nastaju na istoj infrastrukturi kao i njihovi prethodnici, ali dodaju nove opcije i prebacuju mogućnosti više ka samom brauzeru. Ovo dovodi da sa jedne strane postoje novi načini napada na sajtove napravljene novim tehnologijama, a sa druge se na sigurnost starih tehnologija (koje se i dalje koriste) manje obraća pažnja. Često kompanije pokušavaju da se brzo prilagode novim tehnologijama ne razmišljajući o potencijalnim sigurnosnim posledicama. Takođe, ove tehnologije su nove za stručnjake za bezbednost, čije veštine često nisu dorasle zadatku da u novom okruženju uklone stare ranjivosti.

Još jedna mana novog okruženja je da ono menja tradicionalnu dinamiku procesa. Kod tradicionalnih veb aplikacija svi procesi se dešavaju na mreži, tj. serverima sa bazom podataka i onda se šalju prema veb brauzeru koji ih prikazuje. Tehnologije kao što su AJAX i RIA mogu da se upotrebe tako da neke procese prepuste samom brauzeru i ovo omogućava običnom korisniku da vidi te procese i da proučava sam kod. Ovako osetljive informacije su sada dostupne i hakerima.

14.2 SSL enkripcija

Secure Socket Layer predstavlja enkripciju kanala između veb brauzera i servera stvorenog od strane kompanije NetScape.

Najveća društvena mreža Facebook ima delimičnu SSL enkripciju i potencijalna je meta sajber kriminalaca. Hakeri mogu pomoću tehnike *session hijack* češće nazvanu *sidejacking* ukrasti tuđ kolačić – *cookie* preko brauzera. U kolačiću se nalaze informacije o šiframa i korisničkim imenima koje korisnik za određene stranice koristi i ne mora svaki put da ih upisuje kad posećuje stranicu. Delimično preuzimanje kolačića – *partial sidejacking* omogućava napadaču da se uloguje u profil korisnika bez ponovnog upisivanja šifre i korisničkog imena, ali ne daje pristup celokupnom nalogu. Kompletno preuzimanje kolačića – *full sidejacking* omogućava hakeru da pristupi svim stranicama Facebooka-a, ali ne i da vidi tačno koja je šifra ili korisničko ime. Klasičan primer *sidejacking*-a je ekstenzija brauzera Firefox nazvana Firesheep.

14.3 Pecanje preko HTML-a

Pecanje se prilagođava novim stranicama i širi se preko socijalnih mreža zlonameran softver. Preko sigurnosnih obaveštenja prethodno navedenih socijalnih mreža, neželjene elektronske pošte koja ima inficiran PDF dokument i HTML dodataka sa zlonamernim JavaScript-om se ova tehnika koristi. Socijalne mreže imaju sve više korisnika gde su često potpuni stranci prijatelji i lake su mete za napadače. Kada korisnik svom prijatelju pošalje link sa opasnim kodom, ovaj će to isto uraditi i tako se stvara piramida zlonamernog softvera.

14.4 Cross site scirpintg (XSS)

XSS je tehnika ubacivanja skripte u Internet stranicu gde se zluopotrebljava sigurnosna rupa u nekoj veb aplikaciji. Sledeća faza napada može ići preko tehnike *clickjacking* gde se korisnik pokušava prevariti da klikne na deo stranice za koje se navodi da obavlja jednu funkciju, dok u suštini obavlja neku sasvim drugu.

Tokom 2010. Facebook je inficiran koristeći grešku u JavaScriptu. Rezultat je bio da su korisnici bez svoje volje označili da im se sviđa određena Facebook stranica (popularno *lajkovali*) i onda se ta informacija postavljala na zidove svakog korisnika.

14.5 Third-party aplikacije i socijalna manipulacija kod Facebook-a

Third-party aplikacije su vrsta softvera za višekratnu upotrebu napravljenog da bude ili besplatan ili za prodaju od strane nekog drugog entiteta u odnosu na originalnog proizvođača platforme za koje se taj softver pravi. Prednost je što su ovakve aplikacije uglavnom besplatne i ima ih jako mnogo, ali je problem što se one ne moraju stvarati po nekom određenom standardu i zbog toga mogu biti nepouzdanе u radu ili sa velikom mogućnošću zloupotrebe.

Administratori Facebook-a su od 1. juna 2010. godine uveli novi API (Application Programming Intefrace – interejis za programiranje aplikacija) nazvan OAuth 2.0 koji opslužuje sve *third-party* aplikacije na toj socijalnoj mreži. Novi sistem koji je još uvek pod razvojem ima svoje sigurnosne

rupe i kao takav je više ranjiviji u odnosu na prethodni API. XSS tehnika se na novom sistemu mnogo teže može primeniti u odnosu na prethodni sistem, ali samo ako je aplikacija zaštićena u odnosu na XSS. Ako se malo pretaži Internet, naći će se preko 9000 *third-party* za Facebook koje su označene kao ranjive na XSS tehniku.

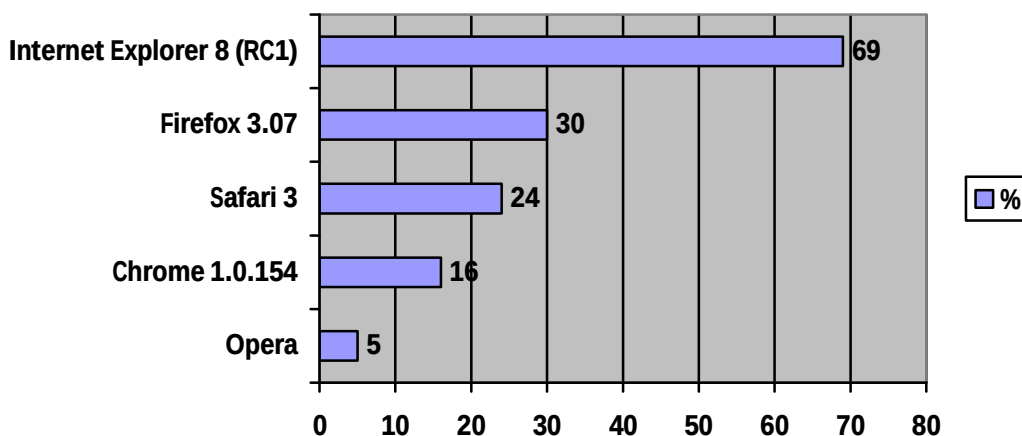
Ranjivost koja postoji kod ovih aplikacija iskorišćavaju sajber kriminalci radi prodaje lažnih antivirusa i drugih programa koji se nazivaju *scareware*. Lakoća povezivanja sa nepoznatim ljudima olakšava korišćenje trikova socijalne manipulacije. Preko *third-party* aplikacija kriminalci reklamiraju svoj zlonameran softver i u njih ubacuju opasan kod.

15. Komparativna analiza pet veb brauzera

Kompanija za Internet istraživanje NSS Labs je od 2009. godine izvršila tri velika testa zaštite veb brauzera od zlonamernog softvera koristeći Live Testing metodologiju, tačnije direktnom pristupu Internetu. Kod svakog testiranja svakog dana je dodavan određen broj stranica. Lista URL-ova sa zlonamernim programima je sačinjena od ogromne baze neželjene pošte sa linkovima ka inficiranim stranicama, i NSS Labs sarađuje sa drugim nezavisnim istraživačima i kompanijama za Internet bezbednost koji im daju pristup dodatnim URL-ovima. Testovi su uključivali ponašanje brauzeru pri posećivanju stranica inficiranim zlonamernog softvera nastalog socijalnom manipulacijom i pecanjem.

15.1 Prvi test – socijalna manipulacija

Za prvi, izvršen tokom prvog kvartala 2009., obuhvaćeno je 5,149 stranica i test je trajao neprekidno 12 dana. Rezultati su sledeći:



Grafikon 1.5 – Uspesnost otkrivanja štetnih programa na prvom testu

Prema NSS Labs-u IE je najubedljiviji sa 69% uspešnosti otkrivanja i iako je testirana pred-finalna verzija Release Candidate 1 (RC1), prema NSS Labs-u brauzer je bio stabilan i samo se nekoliko puta srušio bez trajnih posledica, dok Firefox ima dosta manji procenat u otkrivanju.

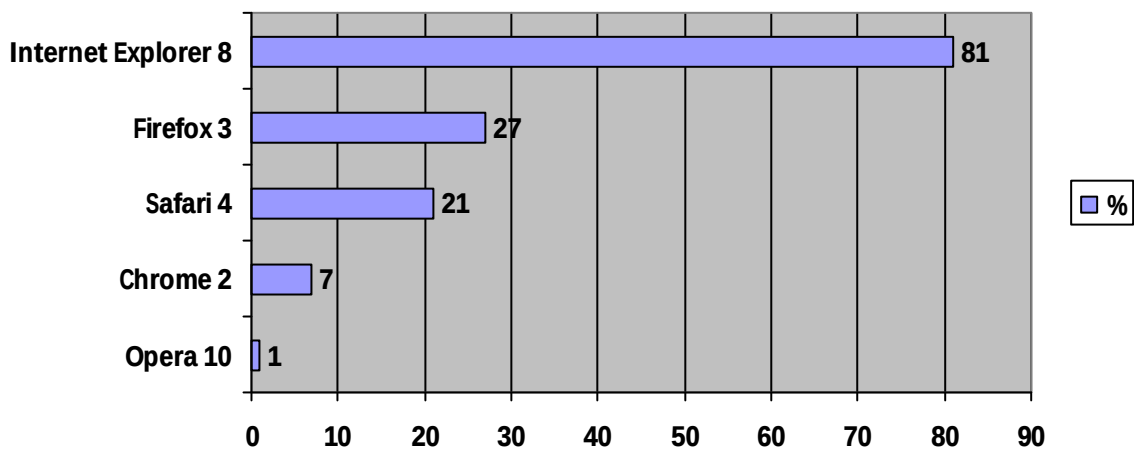
Safari, iako solidnih 24% uspešnosti, ima neaužuran razvojni tim koji retko osvežava podverzije programa i bezbednosne alate i na taj način ostavlja svoje korisnike nezaštićene duže vreme. Takođe se konstantno urušavao dok se brzina testa nije smanjila na 10-15 sekundi između stavljanja stranice na test. Onda je radio stabilno i otkrivanje je dostiglo solidnih 24%.

Chrome je na početku testiranja imao rezultate blizu Firefox-a i Safarija, ali kako je test odmicao, tako su se rezultati drastično smanjili na 16%. Vrlo često se bez razloga gasio, ali ipak je testirana prva verzija i ovaj brauzer je mlađi od svih ostalih.

Opera sa svojih 5% po ovom testu praktično nema odgovarajuću zaštitu.

15.2 Drugi test – socijalna manipulacija

Rađen iste dužine kao i prethodni i sa sličnim brojem stranica:

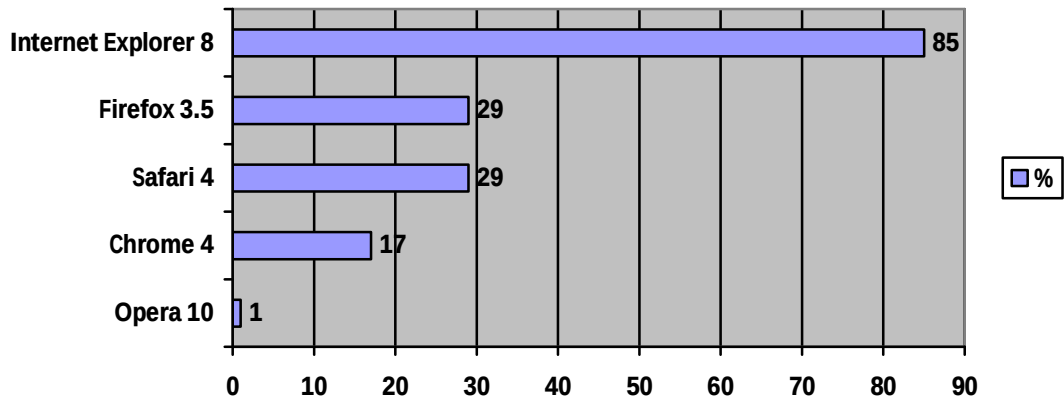


Grafikon 1.6 - Uspešnost otkrivanja štetnih programa na drugom testu

Prema NSS Labs-u Finalna osma verzija IE-a je ostvarila napredak od 12% u odnosu na prethodni test, dok su svi ostali brauzeri imali manje procenata uspešnosti. Firefox 3 manje za 3%, Safari 4 takođe, Chrome sa novom verzijom 2 čak 9% manje uspešnosti, dok je Opera na nivou statističke greške i praktično bez zaštite od socijalne manipulacije.

15.3 Treći test – socijalna manipulacija

Izvršen je istom metodologijom kao prethodna dva testa i trajao je takođe 12 dana:

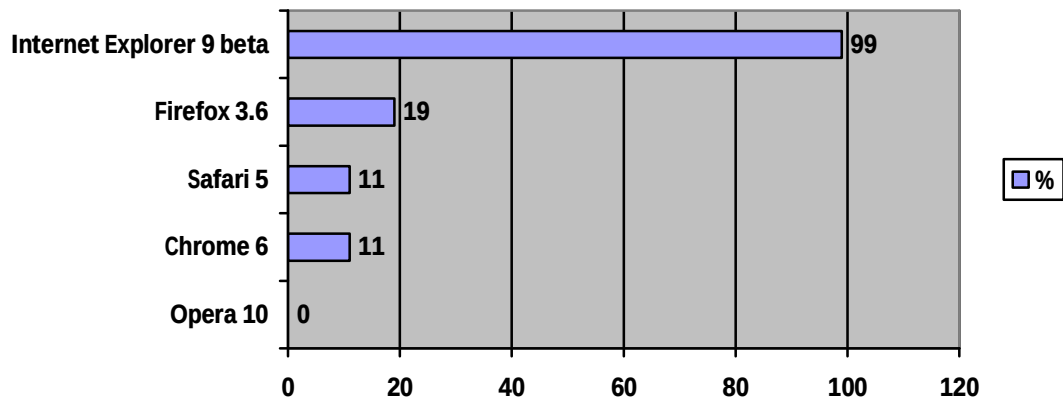


Grafikon 1.7 - Uspešnost otkrivanja štetnih programa na trećem testu

Prema NSS Labs-u IE 8 je ubedljivo najuspešniji sa 85% i povećanjem od 4%, dok su Safari 4 i Firefox 3.5 na drugom mestu sa po 29% uspešnosti. Chrome 4 u odnosu na prethodni test i verziju 2 ima napredak od 10%. Opera 10 ima iste rezultate kao i u prošlom testu.

15.4 Četvrti test – socijalna manipulacija

Radjen je na isti način kao svi prošli testovi i trajao je 11 dana:

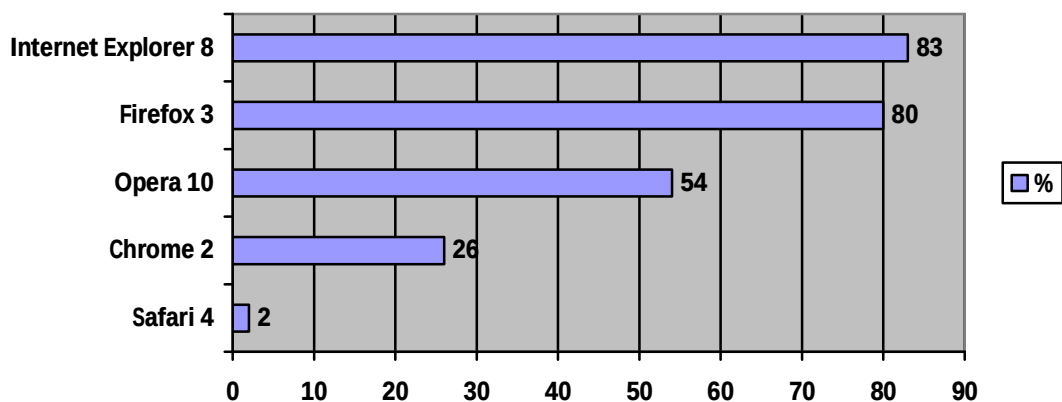


Grafikon 1.8 - Uspešnost blokiranja zlonamernog softvera na četvrtom testu

Ukupan rezultat trenutne verzije IE, verzije 9 beta je skoro potpun. Firefox 3.6 ima relativno slab procenat, 19%, Safari 5 je ostvario 18% manje nego na prošlom testu, dok Chrome 6 ima 14% manje. Opera nema nikakvu zaštitu.

15.5 Test na metodu pecanja

Jula 2009. je izvršen prvi test na zaštitu brauzera od pecanja i trajao je 14 dana:



Grafikon 1.9 - Uspješnost blokiranja zlonamernog softvera putem pecanja

Razvojni timovi Mozilla-e i Microsoft-a imaju trenutno najbolje alate ugrađene u svoje brauzere. Prema NSS Labs-u Firefox 3 ima uspješnost blokiranja 80%, dok IE8 ima 3% više. Opera je na trećem mestu sa 54%, dok Chrome ima uspješnost od 26%. Safari 4 je poslednji sa jako slabim učinkom i na MAC OSX-u i Windows-u.

Zaključak

Celo istraživanje je finansirano od strane Microsofta, koji stoji iza brauzera Internet Explorer. Iako se nakon ove informacije može posumnjati u tačnost rezultata, ovo je jedino istraživanje do sada ovako temeljno urađeno i sa ovolikim brojem inficiranih stranica pomoću kojih su se testovi izvršavali. Na Internetu nisam pronašao nijedno drugo istraživanje koje je uključivalo svih pet najaktuelnijih i najrasprostranjenijih brauzera trenutno na tržištu.

15.6 Istraživački rad

Pri istraživanju pronađene su još neke potencijalno inficirane stranice. Na stranici <http://research.zscaler.com/2010/06/new-fake-av-pages.html> nalazi se objašnjenje o povećanom broju stranica koji se manipulacijom pretraživača stavljaju na prva mesta rezultata nekog pojma. Stranica koja sadrži opasan softver i listu mnogih takvih stranica je: porntube-nowx.com. Pri poseti ovog sajta preko brauzera Firefox, Chrome i Safari, pojavilo se upozorenje o potencijalnoj stranici koja sadrži opasan softver. Kad se pristupilo stranici preko IE-a i Opere stranica je okarakterisana kao nepostojeća. Brauzeri koji se povezuju na crne liste od Google-a

vide tu stranicu kao potencijalno opasnu, dok IE koji koristi svoj SmartScreen Filter i Opera koja se povezuje na GeoTrust kompaniju nije otkrila potencijalnu opasnost nego je stranicu prikazala kao nepostojeću.

Stranice <http://namegamestore.cn> i <http://turbonamestore.cn/> sadrže *iframe* kod sa trojancem i tehnika upada je Drive-by download. Firefox je izbacio upozorenje, dok su svi ostali prikazali stranicu kao nepostojeću.

16. Pravci istraživanja kod predstojećih verzija brauzera

16.1 Mozilla Firefox

Razvojni tim Mozille je za novu verziju njihovog brauzera, verziju 4, pripremili novi sloj sigurnosti *Content Security Policy* (CSP) koji pomaže u otkrivanju nekih vrsta napada, kao što su *Cross Site Scripting* (XSS) i tehnike *drive-by download*.

16.2 Opera

Najnovija verzija kombinuje dva servisa za zaštitu od zlonamernog softvera. Prvi predstavlja prikaz reputacije posećenog sajta, koji se oslanja na prikupljene informacije o tome koliko je taj sajt bezbedan. Drugi servis je skup alata protiv pecanja – Fraud Protection i protiv zlonamernog softvera – Malware Protection. Ovi alati su dostupni od verzije 9, ali od poslednje verzije poboljšavaju sigurnost ovog brauzera, jer su u kombinaciji sa novim servisom, servisom reputacije posećenih stranica.

16.3 Apple Safari

Prve četiri verzije ovog brauzera nisu imale adekvatnu zaštitu protiv bilo kakve vrste zlonamernog softvera. Od nove verzije, verzije 5, razvojni tim Apple kompanije je ubacio alat XSS Auditor, alat sličan onom koji se koristi kod Firefox-a. Ovim je poboljšana zaštita protiv *corss site scripting* tehnike upada u računar preko brauzera.

16.4 Internet Explorer

Drive-by download je jedna od najčešćih tehnika širenja zlonamernog softvera u poslednjih nekoliko godina i zasniva se na zloupotrebi ranjivih delova memorije brauzera preko JavaScript-a. Microsoft, kompanija koja stoji iza Internet Explorera, radi na novom alatu nazvanom Zoozle koji se može ugraditi u brauzer i otkriti ovu vrstu zlonamernog softvera.

Zoozle je uglavnom statičan alat koji može da analizira određenu stranicu i otkrije da li u njenom kodu postoji opasni kod, poznatiji kao *heap spray object*. Zoozle se integriše u brauzerov JavaScript da bi sakupljao podatke iz JavaScript koda koji je pokrenut i da bi alat bio efikasan mora biti isprogramiran tako da može da prepozna one klasične i najčešće elemente opasnog JavaScript koda. Prema istraživačima Microsofta, tehnika zvana Noozle koja skenira milione sajtova i skuplja informacije o opasnim kodovima inficiranih sajtova. Ove se informacije ubacuju

u Zoozle i tako se ovaj alat “uči” da otkriva opasan kod. Nakon prvih rezultata pokazalo se da Zoozle vrlo malo usporava izvršavanje JavaScript koda, što je direktno srazmerno brzini učitavanja takvih stranica.

Zoozle je još uvek u eksperimentalnoj fazi i zvanično se ne planira javna upotreba, međutim kako se tržište brauzera povećava, Microsoft će verovatno ovaj alat ubaciti u finalnu verziju brauzera, IE 9.

16.5 Google Chrome

U nekoliko poslednjih verzija, razvojni tim Google-a proizvodi i ubacuje novu tehnologiju – *Sandboxing*. Flash je najrasprostranjenija vrsta kodeka koja se koristi za strimovanje videa preko brauzera (tačnije preko plug-in dodatka), stvorenog od strane kompanije Adobe. Plug-in-ovi su potencijalna sigurnosna rupa i *sandboxing* izoluje inficiranu stranicu i ne dozvoljava zlonamernom softveru da se proširi na ostale delove računara.

Zaključak

Stvaranje zlonamernog softvera od strane napadača, hakera, organizovanih kriminalnih grupa sa jedne strane i odbrana pomoću specijalizovanih alata razvojnih timova brauzera i stručnjaka za Internet bezbednost sa druge, nikad se neće završiti. Što je više različitih vrsta usluga, više stvari koje ljudi obavljaju češće preko Interneta nego uživo, sve je više potencijalno zaraženih, inficiranih stranica koje mogu ozbiljno oštetiti korisnike na sve više načina. Razvojni timovi brauzera moraju vrlo često, ponekad i svakih nekoliko dana, da osvežavaju svoj brauzer radi ispravljanja sigurnosnih grešaka prethodne verzije. U prvim verzijama većine prethodno istraženih brauzera bila je slaba zaštita od zlonamernog softvera, ali poslednjih godina razvojni timovi stvaraju bolje alate koji služe za otkrivanje i sprečavanje zlonamernog softvera.

Najveći problem ovog dela IT industrije je taj što je njihov svaki korak je preduhitren od strane hakera, napadača i njihovih finansijera (organizovani kriminal), jer su mogućnosti za stvaranje štetnih programa velike i alati za njihovu lakšu proizvodnju dostupni skoro svakome koji ima naprednije programersko znanje. Kad se nađe rešenje za postojeći virus, tehniku ubacivanja štetnog programa preko brauzera ili tehniku socijalne manipulacije, uveliko već napadači izbacuju neku novu verziju zlonamernog softvera za koju u tom trenutku ne postoji odgovarajući način za otkrivanje.

Kako je novac osnovni razlog, mete napada su finansijske institucije, obični korisnici radi, na primer krađe računa u banci, poslovni korisnici najčešće visokog profila, ali i socijalne mreže radi krađe identiteta.

Različitim pristupima (zakonodavnim, socijalnim i tehnološkim) države i kompanije i organizacije za Internet bezbednost troše ogromnu količinu novca i resurse u istraživanja, eksperimente, stvaranje antivirusnih programa i alata za brauzere i tehnika koji otkrivaju zlonamerne programe, propagandnim materijalima za upozoravanje i osveščivanje korisnika, u donošenje novih (nažalost, često nedovoljno dobrih) zakona protiv nelegalnog softvera. Sve ovo može doneti veći broj radnih mesta i dinamiku IT industrije i to je jedina dobra strana pojave zlonamernog softvera. Loših strana ima mnogo više i one se ogledaju u konstantnu bojaznost običnih korisnika socijalnih mreža i kompanija koje prave sopstvene profile (i jednih i drugih je sve više) da neko može ukrasti njihove šifre i kompromitovati njihov identitet na mreži. Mogu doći do privatnih informacija i iskoristiti radi ucene ili na neki drugi način. Finansijske institucije mogu ostati bez svojih klijenata ako neko nelegalno upadne u njihove sisteme i ukrade novac. Svi korisnici Interneta su podjednako ugroženi.

Da li će u narednom periodu biti sve više nelegalnih programa i sve što uz njih ide ili sve manje, zavisi pre svega od društava različitih država i IT industrije i njihovoj smelosti da vide kolika je opasnost sve većeg nereda u najvećoj informatičkoj mreži - Internetu.

Literatura

- [1] http://en.wikipedia.org/wiki/Browser_wars
- [2] http://en.wikipedia.org/wiki/Google_Chrome
- [3] http://en.wikipedia.org/wiki/Internet_Explorer
- [4] http://en.wikipedia.org/wiki/Opera_%28web_browser%29
- [5] <http://en.wikipedia.org/wiki/Firefox>
- [6] http://en.wikipedia.org/wiki/Safari_%28web_browser%29
- [7] http://www.theregister.co.uk/2009/06/09/apple_security_suggestions/http://www.infoworld.com/d/security-central/apples-safari-browser-likened-malware-485
<http://blog.ghostinthemachines.com/2010/05/20/google-chrome-protects-against-malware/http://blog.chromium.org/2008/11/understanding-phishing-and-malware.html>
- [8] <http://www.zdnet.com/blog/security/mozilla-firefox-hit-by-malware-add-ons/5408?tag=content;search-results-rivers>
- [9] <http://www.techspot.com/news/32739-new-firefox-malware-attempts-to-steal-passwords.html>
- [10] <http://www.inquisitr.com/10711/firefox-malware-threat/>
- [11] http://www.computerworld.com/s/article/9062798/Mozilla_raises_Firefox_security_bar
- [12] http://threatpost.com/en_us/blogs/mozilla-admits-malware-sneaked-firefox-add-ons-020510
- [13] <http://www.worldstart.com/tips/tips.php/3183>
- [14] <http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-iii-smartscreen-filter.aspx>
- [15] <http://visualstudiomagazine.com/articles/2010/09/15/microsoft-points-to-ie-9-security-measures.aspx>
- [16] <http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/smartscreen-filter>
- [17] <http://www.eweekeuropa.co.uk/news/zero-day-flaw-in-internet-explorer-exploited-in-spam-attack-11103>
- [18] <http://www.opera.com/browser/tutorials/security/fraud/950/>
- [19] <http://www.opera.com/press/releases/2006/12/18/>
- [20] <http://en.wikipedia.org/wiki/Adware>
- [21] http://en.wikipedia.org/wiki/Computer_virus
- [22] http://en.wikipedia.org/wiki/Ransomware_%28malware%29
- [23] <http://en.wikipedia.org/wiki/Crimeware>
- [24] http://en.wikipedia.org/wiki/Computer_worm
- [25] <http://en.wikipedia.org/wiki/Spyware>
- [26] <http://en.wikipedia.org/wiki/Rootkit>
- [27] http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29

- [28] http://blogs.cisco.com/security/a_brief_history_of_malware_obfuscation_part_1_of_2/
- [29] http://blogs.cisco.com/security/a_brief_history_of_malware_obfuscation_part_2_of_2/
- [30] https://secure.nai.com/us/local_content/white_papers/partners/ds_wp_telconote.pdf
- [31] <http://www.iseclab.org/papers/driveby.pdf>
- [32] http://www.usenix.org/event/hotbots07/tech/full_papers/provos/provos.pdf
- [33] <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf>
- [34] http://en.wikipedia.org/wiki/Farooq_Alvi_Brothers
- [35] <http://www.guardian.co.uk/technology/2008/apr/03/security.google>
- [36] <http://www.realtime-websecurity.com/audio/Podcast-5AntiPhishing.mp3>
- [37] http://en.wikipedia.org/wiki/Social_engineering_%28security%29
- [38] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html
- [39] <http://sixrevisions.com/web-development/the-history-of-web-browsers/>
- [40] <http://en.wikipedia.org/wiki/WWW>
- [41] <http://www.websense.com/content/threat-report-2010-introduction.aspx>
- [42] http://hakin9.org/app/files/download?attachment=attachment1&model=Article&model_id=13580&portal_id=109
- [43] http://www.antiphishing.org/reports/apwg_report_q2_2010.pdf
- [44] http://en.wikipedia.org/wiki/Web_2.0
- [45] <http://www.nsslabs.com/assets/noreg-reports/NSSLabs%20Browser%20Security%20Test%20-%20Socially%20Engineered%20Malware%202009Q1.pdf>
- [46] <http://www.nsslabs.com/assets/noreg-reports/NSSLabs%20Browser%20Security%20-%20Phishing%202009Q3.pdf>
- [47] <http://www.nsslabs.com/assets/noreg-reports/NSSLabs%20Browser%20Security%20-%20Socially%20Engineered%20Malware%202009Q3.pdf>
- [48] http://www.nsslabs.com/assets/noreg-reports/NSSLabs_GTRBrowserSEM_FINAL%202010Q1.pdf
- [49] http://www.nsslabs.com/assets/noreg-reports/NSS%20Labs_Q32010_Browser-SEM.pdf
- [50] <http://www.watblog.com/2010/12/03/microsoft-research-working-on-new-malware-detection-tool-zozzle/>
- [51] https://developer.mozilla.org/en/Security/CSP/Using_Content_Security_Policy
- [52] <http://www.apple.com/safari/features.html#security>
- [53] <http://www.eweekeuropa.co.uk/products/opera-11-heats-up-web-browser-race-review-17258>

- [54] <http://blog.chromium.org/2010/12/rolling-out-sandbox-for-adobe-flash.html>
- [55] <http://blog.chromium.org/2010/12/rolling-out-sandbox-for-adobe-flash.html>
- [56] <http://www.antiphishing.org/>