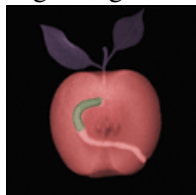


Strahovi računara – apokalipsa na dlanu

Srdan Katić

Dragi čitaoci,

prošlo je neko vreme od kada je izašao poslednji članak iz serijala "Strahovi računara". Više nego očigledno, došlo je do vanrednog stanja u pogledu "zdravlja" Interneta. Gotovo da ne



postoji ni jedan računar sa pristupom Internetu koji je prošao neozleđeno od strane Sobiga, Welchia-e ili Blaster-a. Ni sam ne znam koliko sam vremena proveo čisteći ove trojanke i crve, pokušavajući da pronađem sumnjive tftp fajlove i autoupdate unose u registrima. Sve u svemu možemo reći da se radi o do sada najfrekventivnijoj i najintezivnijoj epidemiji na Internetu. Siguran sam da ste od poslednjih "Strahova računara" sa svih strana bili više nego obasipani sa člancima koji se bave ovom tematikom i koji vam nude rešenja za vaš welchia i blaster problem. Stoga, u ovom izdanju Strahova računara osvrnućemo se na "off-line" dešavanja i pokušati da saznamo šta svet trenutno čini da bi se odbranio od pojave novih virusa i pronašao krivce koji su odgovorni za širenje elektronskih infekcija.

NEK' SE DECA IGRAJU...

Nadam se da su institucije zadužene za sigurnost Interneta shvatile da je izbegavanje elektronskih zaraza poput izbegavanja metaka u Matrix-u. Kompanije neumorno pokušavaju da nađu nove načine odbrane a proizvođači operativnih sistema takozvane zakrpe. Ipak, igra



mačke i miša, gde je mačka obično neki klinac koji nema ni dvadeset godina a milioni korisnika Interneta glume miševu istom, mora da se svede na realne okvire jer, morate se složiti, zvuči pomalo glupo da neko ko se još uvek "loži" na skejtbord i Bad Religion maltretira pola planete i nanosi štete vredne više milijardi dolara. Stoga je bitno iskoreniti izvore ovih zaraza, pronaći krivce i izdizajnirati bolja sigurnosna rešenja. I dalje naravno postoji pitanje etike, da li prema ovim zlonamernim programerima treba biti nemilosrdan ili imati u vidu da su u većini slučajeva u pitanju deca koja ni nisu svesna koji je zapravo efekat onoga što rade već sve podvedu pod "cool" i "trash". U prilog ovoj dilemi ide činjenica da se velika većina hakera nikad ne odluči da unovči svoje veštine i pokrade neku banku ili kompaniju. Kao što je John Malcom, zvaničnik američkog kriminalističkog odeljenja, već rekao mnogi uhapšeni hakeri dožive stres kada se nađu na ispitivanjima i prosto ne mogu da veruju da se njihova krivična dela shvataju tako ozbiljno.

Pitanje koje takođe treba uzeti u obzir je da je pisanje virusa hobi ne samo organizovanih grupa programera hakera (kao što je slučaj sa Sobig organizacijom) već se u većini slučajeva dešava da programeri samostalno krenu da pišu elektronske infekcije, uglavnom koristeći lako dostupne popularne kodove i na taj način stvarajući nove verzije aktuelnih virusa, crva i trojanaca. Ovakvi izvori infekcija, koji ne mogu da se podvedu pod određenu organizaciju

Omega magazin



OMEGA

programera o kojoj se već ponešto zna, zapravo predstavljaju najveću opasnost jer su nepredvidivi i nisu uključeni u standardne tokove hakerskog sveta. Kao što jedan od predstavnika kompanije Counterpane Internet Security i autor knjige "Beyond Fear" Bruce Schneier kaže "Skoro je nemoguće uhvatiti bilo koga od ovih momaka, moralo bi da vam se zaista posreći". U prilog ovoj izjavi ide i činjenica da do sada nije izvedeno ni jedno hapšenje autora virusa koje se nije baziralo na naivnim propustima istog. Autor dobro poznatog virusa Melissa iz 1999. godine, David Smith iz New Jersey-a, je npr. sebe odao tako što je u kodu virusa koristio nadimak svoje devojke a pri inicijalnom slanju zaraženih poruka koristio nick-ove koji su kasnije uspešno upoređeni sa njegovim nadimcima na raznoraznim forumima i mejling listama.

U Omega vestima ste ranije mogli da pročitate da je 19. avgusta ove godine uhapšen osamnaestogodišnji Jeffrey Lee Parson iz Minesote koji je sebe odao na sličan način tako što je ostavio svoj "online" alias u kodu infekcije. U hapšenju mladog Parsona učestvovalo je čak 30 agenata Američke tajne službe (koliko je tek bilo obično policije?!) a u njegovoj kući



je pronađeno i zaplenjeno čak 7 personalnih računara! Pored činjenice da je Parsonov crv sadržao očigledan dokaz o identitetu autora, FBI stručnjacima je trebalo čak 3 nedelje da nađu krivca! Zvanično objašnjenje za ovaj propust u istrazi se bazira na priči tipa "ko je mogao da očekuje da je neko tako glup" a komičnost tronedeljne istrage koju je vodio sam vrh države pojačava i činjenica da je bilo ko putem Google pretraživača mogao da otkrije Parsona od samog starta, jedino je bilo potrebno da ukucate reč "teekid" u Google-u i pojavio bi se Parsonov lični web site, sve skupa sa kućnom adresom i brojem telefona. Parson je optužen za kreiranje varijante Blastera pod imenom Blaster.B (LovSan) koja je počela da se širi 13. avgusta ove godine, samo dva dana nakon pojave originalnog blaster crva čijem autoru ni jedna organizacija za sigurnost Interneta nije na tragu. Parson se izjasnio kao nevin po optužbi koja ga tereti "da je sa namerom izazvao štetu zaštićenih računara" (prim. prev.) a suđenje ovom tinejdžeru počinje 17. novembra 2003 godine u Seattle-u. Glavna odbrana Parsona leži u banalizovanju njegove namere jer su mu na računaru pronađena samo 3 američka dolara a ako mu to ne prođe kao olakšica najverovatnije ga čeka kazna do 10 godina zatvora.

Ubrzo nakon hapšenja Parson-a rumunska policija je uhapsila 24-godišnjeg rumunskog hakera koji je optužen za kreiranje F. Vajante blastera. Rumunski haker je kreirao verziju blastera koja je "upakovana" u izvršni faj enbiei.exe. Kako su stručnjaci utvrdili (kad nemaju Vuka da im lepo kaže) radi se o fonetičkom izgovoru skraćenice NBA koja nam je svima dobro poznata. Dalje, optuženi je koristio identičan nadimak na chat kanalima i time sebe još više razotkrio. U najgoroj situaciji od svih ovaj haker se može suočiti sa kaznom zatvora do 15 godina. Rumunija je inače nedavno donela zakon o borbi protiv sajber kriminala i pisanja zlonamernog softvera.

Jedino preostalo ovogodišnje hapšenje kojim se bilo ko može pohvaliti je hapšenje dvojice Britanaca koji se terete da su "stvorili zaveru koja je imala za efekat da vrši neautorizovane modifikacije sadržaja na računarima sa namerom nanošenja štete u pogledu operativnosti istih" (prim. prev.). Naime, optuženi su kreirali Troj/TKBot.A napast.

Omega magazin



OMEGA

Nažalost, nijedan ovogodišnji uhapšenik nije "velika zverka". Kao najpopularniji od svih, tinejdžer Parson je kreiranjem svoje verzije blaster ugrozio oko 7.000 računara. Ako uzmemo u obzir da je nepronadeni autor originalnog blaster koda ugrozio preko 500.000 računara onda možemo slobodno zaključiti da je Parson samo sitna riba i da hakerski boss još uvek mirno spava. Jedan od razloga zbog koga je Parson stekao ovu nepriželjkivanu popularnost je poruka koju je ostavio u samom kodu a koja je namenjena Bill Gates-u i koja glasi "bill gates why do you make this possible? Stop making money and fix your softver!" Moramo priznati mladom Parsonu da je prilično jasno i konkretno argumentovao svoju poruku.

Još vam je jasniji očaj situacije kada čujete da je direktor Symantec-ovog istraživačkog centra Vincent Weafer dao pesimističnu izjavu "da od 5 do 15 novih virusa, koliko se dnevno pojavi na Internetu, skoro ni jedan autor neće nikada biti uhvaćen". "Čak i ako ih uhvate" - navodi Vincent Weafer – "to ne mora da znači da će završiti u zatvoru jer u mnogim zemljama kreiranje virusa nije ilegalno", drugim rečima te zemlje nemaju zakon na osnovu koga bi optužile hakere i ostale zlonamerne programere.

Ako je to tako kao što i jeste onda je očigledno da klasične detektivske "fore" ne pale baš mnogo i da su pravila igre u borbi protiv hakeraja sasvim drugačija od standardnih jer predstavljaju borbu protiv sasvim novog oblika kriminala u svetu koji ne poznaje fantom maske i pretnju oružjem.

ŠTA NAS MUČI?

Povodom invazije virusa i crva 10. septembra ove godine održan je "US Congressional hearing" skup koji se bavio pitanjem sigurnosti Interneta u novonastaloj situaciji navale elektronskih crva i virusa. Mesec avgust 2003. godine je bio najgori mesec u istoriji sigurnosti informatičkih sistema, bar ako sudimo po statistikama MiG2 instituta u Londonu koji ovakve i slične statistike objavljuje još od 1995. godine. MiG2, Londonska kompanija za procenu digitalnog rizika, objavila je da ekonomska šteta nastala tokom avgusta ove godine od virusa i hakerskih delatnosti iznosi 32.8 milijardi dolara. Sam Sobig je pak uspeo da se približi ovoj cifri i načini 29.7 milijardi dolara ekonomske štete u celom svetu. Posle ovakvih cifri nije ni čudo što su kongresnom skupu prisustvovali najviši predstavnici vodećih sila u IT svetu. U pitanju su rukovodioci kompanija poput Network Associates, Symantec, Microsoft, Cisco, VeriSign a takođe i predstavnici samog State Department-a. Predloženi su koraci koji bi uticali na bolju edukaciju dece u oblasti računarske etike i na finansiranje računarskih sudskih timova. Jedan od zanimljivijih i uvaženijih predloga je bio predlog predsedavajućeg podkomiteta, Adam-a Putnam-a, da se kreira takozvana sajbersigurnosna lista (cybersecurity checklist) koju bi kompanije koje javno nastupaju preko Interneta morale da popune. Naime, radi se o zakonski propisanoj listi sigurnosnih rešenja koje bi navedene kompanije morale da popune navodeći time koje od stavki imaju implementirane u svojim mrežama. Na taj način bi ovakve kompanije više pažnje posvetile pitanju sigurnosti informatičkih sistema iz prostog razloga što bi nedovoljan broj obeleženih stavki značio u isto vreme nezadovoljstvo i nesigurnost investitora i klijenata. Pa da, savršena ideja, naterajte trgovca da uradi nešto time što ćete zadovoljstvo investitora i klijenata usloviti istim.



Omega magazin



OMEGA
KORAK NAPRED

Dok su Amerikanci raspravljali o progresivnim metodama digitalne zaštite, Britanci su preuzeli prve konkretne korake. Verovatno ste već naleteli na vesti koje se bave novom Britanskom modom u pogledu korišćenja poslovnih računara. U poslednjih godinu dana u Velikoj Britaniji je oko 30% kompanija uvelo novu politiku korišćenja računara na poslu.



Mnogi su ukinuli chat i IRC portove na svojim "firewall" uređajima i uveli filtriranje mejlova kako bi sprečili razmenu slika između zaposlenih i korisnika javne mreže. U strahu od virusa i crva i u želji da povećaju produktivnost zaposlenih kompanije se sve više odlučuju na ove metode mada neki za ovakvu odluku imaju specifičnije razloge od ostalih. Na primer, veliki broj proizvođača automobila se odlučio da uvede filtriranje slika pre svega zbog zaštite privatnosti. Direktori ovih kompanija se plaše da bi putem Interneta zaposleni mogli da odaju poslovne tajne tako što bi slali slike novih modela automobila koji se još uvek nisu pojavili na sajmovima i u prodavnicama. Direktor istraživačkog centra u Clearswift kompaniji koja se bavi proizvodnjom softvera poput e-mail i jpeg filtera tvrdi " da sigurnost nije samo kada sebe zaštitite od spam poruka i virusa, zaposleni su najčešće najslabiji link" i lično mislim da je veoma u pravu. Ukoliko neko kontinuirano posećuje pornografske sajtove ili se svako jutro uz kaficu svađa preko chat-a sasvim je sigurno da će pre ili kasnije pokupiti raznorazne viruse ili će njegov računar biti pretvoren u takozvanog "zombija", računar koji je pod kontrolom nekog hakera. Nebitno je koliko vam je nova definicija na AV softveru ili da li imate "firewall" jer na Internetu uvek postoje "bolesti" za koje trenutno ne postoji lek ili primena postojećeg leka može da ozbiljno degradira poslovanje..

MICROSOFT SE OTVORIO ZA TURU

Još jedan od načina borbe protiv kriminala koji je uvek bio uspešan je nuđenje nagrade za pomaganje u pronalaženju i hapšenju krivca. Kao što ste skoro mogli da pročitate u dnevnim vestima Omega magazina, Microsoft je ponudio 250.000 dolara nagrade onom koji pomogne



u pronalaženju Blaster i Sobig autora i odvojio još 4.5 miliona dolara za buduće "lovce na glave". Da li vam nešto deluje sumnjivo u tome da Microsoft nudi pare? Naravno da postoji veoma veliki razlog za ovaj potez softverskog giganta. Pre svega epidemija virusa je najozbiljnije do sada ugrozila Windows sisteme što je nateralo mnoge da počnu da ozbiljno razmišljaju o OpenSource platformama. Bez dlake na jeziku, kao i uvek, Microsoft je takođe iskoristio priliku da uz pomoć ove nagrade opere ljagu sa sebe, ili bar neki deo iste, "kol'ko se može". Patrick Gray, direktor Internet Security Systems inkorporacije, je na otvaranju Microsoft-ovog Reward programa doslovce aplaudirao pa je stoga više od ostalih novinarima skrenuo pažnju na sebe. Ovaj bivši borac protiv sajber kriminala je pokušao "malčice" da podiđe Microsoft-u pa je izjavio "da smo dosta vremena imali fokus na bagovit softver (pa ko ne bi?!) i da je vreme da prebacimo fokus tamo gde mu i pripada a to su ljudi koji čine ove zločine".

Posle ove izjave se prosto zapitam: "ako mi je Mercedes prodao auto koji nema bravu i za to svi znaju da li je onda krivica nekog klinca što je seo u moj auto i provozao se ne ukraivši ništa ili bi pak trebalo da budem ljut na kompaniju Mercedes?". Ne kažem da bi obožavao

Omega magazin



O M E G A

tog klinca ali sam siguran da bi zasigurno podneo tužbu protiv Mercedesa, pogotovo jer u specifikaciji auta nigde ne stoji bilo kakva informacija o nepostojanju brave koja se sasvim podrazumeva, morate se složiti. Međutim, nisu svi istog mišljenja kao ja. Izvesna Roberta Domres, ponosni korisnik Microsoft proizvoda, je pak na "dam pare za glavu" paradi izjavila da su virusi i crvi akt terorizma i bezkompromisno optužila autore istih". Ako je resetovanje nečijeg računara akt terorizma kakav bi onda akt bio puštanje u promet virusa koji briše sve podatke i krade milijarde dolara iz svetskih banki? Sigurno još uvek ne postoji dovoljno gnusan termin koji bi gospođa Dormer iskoristila da okarakteriše tako nešto mada se mora priznati da niko ne može da garantuje da i sami teroristi ne koriste "crtljive" metode sabotiranja zapadnog sveta, mada za tako nešto ne postoje nikakvi dokazi.

ZAKLJUČAK

Sve u svemu, lepo je što Microsoft nudi nagradu i svakako taj akt valja podržati ali se plašim da bi (bar) nekoliko stotina puta bilo efektivnije da Microsoft pitanje ranjivosti Windows-a reši na nivou samog rešenja Windows arhitekture a ne da "ispravlja krive drine" tako što će da puni zatvore tinejdžerima i tera korisnike da "žive u paranoji" i koriste maksimum 50 % potencijala Windows-a, daleko od onoga što piše na Microsoft pamfletima.



Ipak, šanse da tako nešto desi su minimalne tako da moramo da se oslonimo na zakrpe, ukrpe i pokrpe kojima nema kraja i da se nadamo da elektronske infekcije neće početi da gase aparate za održavanje života po bolnicama. Mnoge kompanije koje se bave analiziranjem sigurnosti Interneta upozoravaju da su trenutno aktuelni virusi, crvi i trojanci najverovatnije samo uvod u veliku katastrofu koja može da se desi svakog časa. Bilo koji od virusa koji nam zarazi računar može da nam obriše sve podatke ili pokrade poverljive informacije. Zamislite samo kako bi izgledalo kada bi nacrti za nuklearno oružje ili izradu smrtonosnog virusa dospeli na Internet, sve skupa sa detaljima i uputstvima. Ako još uzmemo u obzir da je potrebno 30 agenata tajne službe da se uhapsi haker, i to samo ako isti haker napravi budalu od sebe, recite mi onda kolike su onda šanse da uhvatite nekog hakera koji se smatra najboljim i najopreznijim u svojoj struci? Možda je jedino rešenje programom obuke iz oblasti računarske etike edukovati i preusmeriti one koji prave viruse iz zabave i sujete a one koji pak to rade "sa višim ciljem" ne verujem da će iko ikada videti uživo. Iz tog razloga imamo samo dve opcije, da napravimo i koristimo operativni sistem koji je skoro nemoguće izhakerisati (hm...) kako bi se opasnost od katastrofe minimizovala ili da korišćenje i rad Interneta postanu zakonski regulisani što u pogledu upotrebljivosti može da ozbiljno kompromituje Internet kao centar informativnih tokova modernog sveta.