UVODNA REČ

RELJA JOVIĆ

Poplava pecaroša

UBEĐENI STE da će novi „antipecaroški" filtri u Internet Exploreru 7 i Firefoxu 2 zaštititi vaše privatne podatke? Možda je vaš optimizam bez pokrića – „pecaroških" Web lokacija je prošle godine bilo znatno više nego pre, dok je broj Amerikanaca koji su bili žrtve prevarantskih šema skoro udvostručen. U novembru 2006. godine, a to je poslednji mesec za koji su podaci dostupni, Anti-Phishing Working Group je prijavila 37.439 novih „pecaroških" lokacija, što je za 709 procenata više od 4.630 takvih lokacija u novembru 2005. godine.

Prošloga oktobra su Mozilla i Microsoft objavili nove verzije svojih Web čitača koji koriste tzv. crne liste za blokiranje pristupa poznatim prevarantskim lokacijama. Kao odgovor, dobro opremljeni „pecaroši" toliko brzo postavljaju nove lažne Web lokacije da je prosto nemoguće da sve budu zatvorene ili postavljene na crnu listu.

„Uskoro će", upozoravaju stručnjaci, „tehnologije koje se pretežno oslanjaju na crne liste postati beskorisne."

Prema izveštaju kompanije RSA, japanski hakeri prodaju softverski komplet koji omogućava kriminalcima da, uz neznatan trud, postave vrlo ubedljivu lažnu Web lokaciju. Na „lažnjak" se prevlače slike i raspored elemenata na strani s pravе Web lokacije, po pravilu neke banke ili druge finansijske institucije, i onaj se prosleđuju uneti podaci korisnika da bi se „odglumilo" regularno prijavljivanje – ali se kopija podataka o nalogu ili računu čuva za kriminalce.

Cilj je, naravno, veća zarada. Istraživačka kompanija Gartner procenjuje da je prošle godine tri i po miliona Amerikanaca odalo svoje poverljive informacije „pecarošima", što je 84 procenta više nego u istoj godini – ukupan gubitak je bio dve milijarde i osam stotina miliona dolara. Procene kažu da je jedna jedina „pecaroška" banda, poznata kao Rock Phish, zaradila preko sto miliona zelenih novčanica.

Prema tvrdnjama stručnjaka za zaštitu, Rock Phish je primenila nekoliko metoda koji su prouzrokovali dramatično povećanje broja „pecaroških" lokacija u nekoliko prethodnih meseci. „Pronalazak" te grupe su i neželjene poruke sa slikom, koje zaobilaze filtre tako što je zamka ugradena u sliku, upozoravaju stručnjaci. Bilo je dana kada je Rock Phish, specijalizovan za obmanjivanje američkih i evropskih finansijskih institucija, bio odgovoran za najmanje polovinu svih aktivnih „pecaroških" lokacija, naglašavaju istraživači.

Heurističko skeniranje može da pomogne u borbi protiv ove pošasti. Umesto korišćenja crnih lista, analizira se ponašanje lokacije i traga za tehnikama koje prevaranti najčešće koriste. IE 7 obavlja heurističko skeniranje, kao i SiteAdvisor, besplatan dodatak za Internet Explorer i Firefox.

Predloženi standard za novi vid certifikacije lokacija, Extended Validation Secure Socket Layer (EV SSL), verovatno će biti od velike pomoći. Da bi dobile taj certifikat, lokacije će morati da provere nezavisne kompanije kao što su VeriSign i Entrust kako bi se uverile da su u najmanju ruku legitimne. Kada budu odobrene, adresno polje u Web čitaču će biti obojeno zeleno.

Međutim, ako sadašnja poplava „pecaroških" lokacija išta dokazuje, onda je to činjenica da prevaranti mogu da zaobidu automatizovane alatke i procedure kako bi zaštitili svoju priličnu zaradu – i da to uspešno rade. Nedavno su usavršili nove metode koji vrlo efikasno probijaju zaštitne mere kao što je EV SSL, tvrde analitičari u kompaniji Gartner.

Sumnja se da će sertifikati EV SSL imati veliki uticaj na „pecaroške" prevare, jer veruje da kompanije koje se bave zaštitom snose deo krivice za mrežne pretnje.

Industrija zaštite računarskih sistema je bila u izvesnoj meri arogantna jer ljudi ne shvataju koliko su vešti i prefinjeni mrežni kriminalci.

Iako još uvek nije izmišljen čarobni štapić koji bi nas sve zaštitio (a sigurno ga neće ni biti), postoji jednostavan način odbrane od većine „pecaroških" napada. Nikada ne pritiskajte hipervezu u e-poruci ili na nekoj vama nedovoljno poznatoj lokaciji koja bi vas mogla odvesti na stranicu s poljima za unos podataka o finansijskom računu ili nalogu. Ako uvek unosite Web adresu ili koristite sopstvene zabeležene adrese, čak i kada ste stoprocentno sigurni da je e-poruka legitimna, trebalo bi da budete bezbedni.

Besplatne, automatizovane alatke kao što su Password Safe (find.pcworld.com/56483) i Pwdhash (find.pcworld.com/56482) i dalje će vam pružati dragocenu pomoć. Međutim, da biste se efikasno borili protiv „pecaroša", najbolja zaštita još uvek ste – vi sami. ■

Relja Jović je glavni i odgovorni urednik časopisa Mikro. *Njegove uvodne reči pročitajte na adresi www.mikro.co.yu/arhiva/relja.*