



Paris Hilton, pecaroši i prevare

NOVI VID krađe identiteta, tako što se korisnici varaju zloupotrebom brojeva telefona, širi se poput kijavice. O kolikoj se pošasti radi najbolje svedoči skorašnji incident o kom su izveštavali čak i tabloidi.

Žestoka medijska svada između dveju ličnosti koje su u žiži interesovanja javnosti, glumica Paris Hilton i Lindzi Lohan, nedavno je podstaknuta saopštenjem jedne male firme za prodaju nasumičnih telefonskih identifikacionih brojeva. Ta firma je optužila Hiltonovu da je „upala“ u nalog glasovne pošte na neimenovanoj mreži mobilne telefonije.

Hiltonova je jedan od pedesetak korisnika čiji su nalozi povučeni zato što su zloupotrebili uslugu „maskiranja“ identifikacije poziva kompanije SpoofCard.com da bi prodrli u naloge glasovne pošte, tvrde zvaničnici pomenute firme. Mnogi nalozi u koje su izvršeni upadi pripadaju slavnim ličnostima, a među njima je i Lohanova.

Lokacija SpoofCard.com nije zvanično optužila Hiltonovu da je zloupotrebila glasovnu poštu svoje estradne suparnice. Međutim, tračevi o slavnim ličnostima, koji ionako obiluju detaljima o rivalstvu te dve „zvezde“, dopunjeni su i novim.

List New York Post je nedavno obavestio svoje čitaoce da je neko ukrao lozinku za uređaj BlackBerry Lohanove i poslao njenim prijateljima „odvratne i vrlo zle poruke za koje su svi smatrali da potiču od Lindzi“. Njen predstavnik za medije nagovestio je da iza te pakosti možda stoji Paris Hilton.

Hiltonova je bila nedostupna da bi dala svoj komentar, ali je njen predstavnik Elliot Minc izjavio za E! Online da se navodni upad „jednostavno nije ni dogodio“ i da je verovatno neko drugi otvorio nalog na lokaciji SpoofCard.com predstavljajući se kao Paris Hilton.

Mreže mobilne telefonije Cingular Wireless i T-Mobile koriste samo telefonski broj kao identifikaciju za prepoznavanje korisnika glasovne pošte, pri čemu ne zahtevaju ni unošenje lozinke. To znači da su pretplatnici tih mreža bili ranjivi na zloupotrebe usluge SpoofCard, tvrde stručnjaci iz kompanije Secure Science, specijalizovane za bezbednost informacionih sistema.

Opisani skandal ilustruje kako na telefonsku industriju utiče jeftin softver za telefoniranje kao što je, na primer, sistem otvorenog koda Asterisk. Nedavno su „pecaroši“ zloupotrebili taj softver za aktiviranje jeftinih telefonskih mreža koje lažnim porukama e-pošte dodaju notu autentičnosti. U „pecaroškim“ napadima, kradljivci identiteta šalju e-poruke koje po svemu liče na dopise banaka, kompanija koje izdaju kreditne kartice ili usluga mrežnog plaćanja poput PayPal. U poruci najčešće piše da je nalog primaoca bio ugrožen na neki način, i zato se u njoj nalazi hiperveza do Web lokacije, po izgledu skoro istovetne zvaničnoj, na kojoj bi primalac trebalo da unese ispravne lične podatke. U novoj šemi, kradljivci identiteta mole potencijalne žrtve da pozovu broj telefona pridružen VoIP nalogu, a on se lako može dobiti preko mrežnih usluga poput Skypea ili mreže prodavnica koje prodaju VoIP proizvode kao što je Vonage Holdings.

S manje od deset zaposlenih, Spoof-

Card.com je mogao da koristi Asterisk i operativni sistem Linux za poslovanje koje bi pre samo deset godina bilo preskupo. Ta kompanija za deset dolara prodaje telefonske kartice sa 60 minuta kredita koje kupcima omogućavaju korišćenje besplatnog telefonskog broja i unošenje proizvoljnih identifikacionih podataka što se prikazuju na displeju telefona primaoca poziva.

Iako u toj kompaniji tvrde da je korišćenje njenih usluga legalno – jer omogućava, primera radi, da radnici na terenu prikažu brojeve telefonskog sistema svog preduzeća, najnoviji incident doka-



zuje da ta tehnologija širom otvara vrata za zloupotrebe. Pre godinu dana, američki kongresmen Tim Marfi je tvrdio da je bio žrtva nepoznate osobe koja je iskoristila lažnu identifikaciju i ostavila nepodobne poruke, a poticale su navodno iz njegove kancelarije.

Početkom ove godine, američka Savezna komisija za komunikacije je pokrenula istragu o lokacijama za pri-

krivanje i lažno prikazivanje identifikacije pozivaoca. Međutim, prema tvrdnjama upućenih, upadi u glasovnu poštu bi lako mogli da budu sprečeni samo ako bi sve kompanije za mobilnu telefoniju zahtevale i unošenje lozinke. Rešenje problema je, znači, u rukama telekomunikacionih kompanija – dovoljno je da „zaključaju“ svoje sisteme glasovne pošte kao što je to uradila kompanija Verizon i na taj način će ova epizoda pretnji biti okončana, ali ne i čitava serija. ■

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