# Neznosna lahkost skrivanja

**Zdaj pa gre zares. Hudodelcem bomo pošteno stopili na prste! Tako bomo, po tistem, ko že tako učinkovito sezuvamo ljudi na letališčih in jim prežarčujemo računalnike, uvedli še bolj rigorozne ukrepe. Vse šminke in maskare, najučinkovitejša ženska orožja, je treba seveda zelo temeljito nadzorovati. Prav tako otroško hrano, saj vsi vemo, da izgleda kot strup v malih stekleničkah. Lahko pa ljudi na letalo pustimo s starimi dobrimi steklenicami viskija, sploh, ker so prijazno podpirali ekonomijo brezcarinskih prodajaln. Ko bo prvi terorist sesul kak nebotičnik z viskijem, bomo pa vnos na letalo po osebi omejili na 100 ml.**

Teroristi in digitalni kriminalci imajo pravzaprav veliko skupnega. Tako eni kot drugi so zmeraj bolj tu in vplivajo na vedno več vsakodnevnih navad in odločitev malih ljudi. Vsi njihovi uspehi govorijo o tem, da so mojstri skrivanja in da smo pravi cicibani v odkrivanju njihovih namer. Oboji povzročajo vedno večjo denarno škodo, njihov obseg delovanja kaže izredno nevaren trend rasti, ki ga ukrepi, kot so prepoved vnosa otroške hrane na letalo, očitno ne morejo ustaviti.

Kriminalno hekanje ima ob tem še to lepo lastnost, da je odličen in zanesljiv dolgoročen posel - za globalno ribarjenje ocenjujejo, da je bolj dobičkonosno kot prekupčevanje s heroinom, pa še redko jih dobijo. Osem zelenih milijard škode so na FBI v preteklih letih prijavila ameriška podjetja samo zaradi hekerskih vdorov, kar pa predstavlja le dokazljivi in iztožljivi del posla in ne vsebuje kraj informacij ter identitet. Račune za slednje bomo plačevali šele v naslednjih letih, morda v obliki višjih bančnih provizij. Kot vsak dober posel z močnim pospeškom je tudi za tega pričakovati, da ima naravni nagon po rasti in da bo za svoje potrebe razvijal še bolj prefinjene metode skrivanja, ker so katalizator hekerskega uspeha. Nakopičene plačilne kartice, digitalna potrdila, gesla in zaupne informacije po podatkovnih bazah in strežnikih predstavljajo hekerjem koncentrirano moč in izjemen vir zaslužka za prihodnost, zato ne preseneča, da se znotraj te 'industrije' pojavljajo specializacije. Če je bila pred časom na črnem trgu velik hit prodaja 'zaseženih' (owned) računalnikov za pošiljanje neželene pošte, je danes v porasti donosen izsiljevalski trend, ki spravlja na kolena z grožnjami onesposobitve ključnih sistemov ali z razkrivanjem sočnih skrivnosti vplivnih posameznikov.

Čeprav so za uspešnost skrivanja zaslužni napadalci sami, si moramo prav vse minuse za neučinkovitost obrambe pripisati predvsem branitelji. Usodno napako naredimo, ko se preveč zanesemo na lastno sposobnost odkrivanja napadov, ki žal ne deluje posebej učinkovito. Ko nam tat hodi po lastni hiši in se razgleduje za zlatnino, si seveda smemo zaploskati, ko ga opazimo in lastnoročno vržemo skozi vrata, a to drugo pogosto ni tako zelo preprosto. Če se recimo hočemo iz omrežja zanesljivo znebiti rootkitov, bomo morali ponovno namestiti prav vse računalnike. Napadalcem pomaga tudi dejstvo, da je možnih napadov neskončno mnogo, prepoznavamo pa jih le končno veliko. Čeprav jih sistematično dodajamo na seznam znanih napadov, bo le-ta v primerjavi z napadalčevim arzenalom napadov prav boren. In kako bomo v neobvladljivi količini podatkov, ki polzijo v omrežje in nazaj, izločili en sam usodno zamaskiran paket z zlikovsko vsebino, ki izgleda ljubko in nedolžno kot Scarlett Johansson? Nimamo veliko možnosti, šumov iz okolja je preveč. Najslabše pa je, da je nepooblaščeni gost že pri nas in da je veselo stikal po predalih, pri čemer ni puščal nobenih sledi. Če že morda ugotovimo, kam gre, lahko samo nepoučeno ugibamo, kje vse je bil.

V digitalnem svetu se napadalci zelo lahkotno izmuznejo v naša omrežja, saj smo ljudje pri uporabi digitalnih virov vse premalo dosledni in previdni. Tudi programska oprema, ki jo uporabljamo, je zaradi finančnih optimizacij luknjasta in daleč od popolnosti. Če se vsaj malo potrudijo, se hekerji lahko učinkovito skrijejo, poskrbeti morajo le, da niso preveč glasni in da njihove aktivnosti ne spominjajo na vzorce, ki smo jih nekoč zložili na seznam naših znanj in jih poskušamo redno odkrivati. Napade snujejo tako, da vohljajo za pomanjkljivostmi. Svojo nepredvidljivost ter iznajdljivost, ki nam povzročata toliko sivih las, pravzaprav črpajo iz naših napak. Če sistemi, aplikacije, človeško obnašanje in procesi ne bi bili tako dosledno ranljivi, bi bilo uspelih napadov precej manj. Absurdno je, da ljudje delamo po vsem svetu napake podobne vrste, zato si lahko napadalci na črnem trgu poceni kupijo programske pakete za vdiranje in se sami niti ne trudijo z njihovim razvojem.

In zakaj se potem tako malo ljudi odloči, da bi sami preventivno in učinkovito počeli podobno, kot delajo napadalci? Nemarno se branimo iskanja lastnih ranljivosti in to prepuščamo tistim, proti katerim se borimo. Odstranjevanje izvornega greha - ranljivosti – je vendar najučinkovitejši način obrambe, preventiva je cenejša od kurative. Tako naslednjič, ko se boste želeli pohvaliti s tem, da vdorov v vaš sistem še ni bilo, pomislite na neznosno lahkost skrivanja napadalcev. Lahko, da boste povedali več o lastni neuspešnosti odkrivanja napadov kot o deviški nedotaknjenosti vašega omrežja.

Stanka Šalamun, Sistem, dec 2006