Čari interneta

Vsakodnevno širokopipično surfanje zahteva posebno pripravo abaka in na njem naloženega programja. V nasprotnem primeru kaj hitro pride do okužb ali celo kraje podatkov. Kako in s čim se temu ogniti, razkriva doktor Lun(ovsk)i.

Vprašanje internetne varnosti že dolgo ni več tema, s katero se ukvarjajo le računalniški zagrizenci. S prodorom spleta v življenja splošne populacije se je močno razširila zavest o njega nevarnih straneh. O posebej uspešnih virusih in črvih navsezadnje radi obveščajo po poročilih, dnevno časopisje nemalokrat gosti članke na temo maliciozne kode, o zaščiti omreženih kompov se pogovarjajo po radiu ... Bombardiranje z vseh strani je nedvomno koristno, saj zmanjšuje število morebitnih žrtev. A po drugi strani med (največkrat) nevednim ljudstvom ustvarja pravo grozo do vsega internetnega. Poznam osebke, ki iz strahu pred za slehernim vogalom prežečimi virtualnimi bavbavi net uporabljajo le za kratek čas, in še to le takrat, ko res ne gre drugače. Še neprimerno več je takih, ki zavračajo vsako možnost uporabe kreditne kartice za internetne nakupe, kaj šele, da bi pomislili na spletno bančništvo. Tovrsten odnos kajpak najbolj škodi ravno njega lastnikom, saj je net za sodobnega človeka nujen del vsakdanjika. Odpovedati se mu vsled slonov, ki so v resnici miši (ali, v najslabšem primeru, dobro rejeni psi), je povsem kontraproduktivno. Čeprav drži, da so mrežna prostranstva polna nepridipravov in pasti, jih je moč s par programčki, nastavitvijo ali dvema in predvsem s trezno glavo obiti v veliki meri, če že ne docela. Ogledali si bomo, kako.

Toda pričujoči spis ni namenjen le začetnikom. V njega prebiranje vložene minute bodo prav prišle tudi tistim, ki internet jemljejo kot nekaj samoumevnega in se v njem znajdejo kot ribe v vodi. Kot me je nedavno podučil izredno spretno zamaskirani MSNjevski črv, je totalna varnost utopija. Podcenjevanje sposobnosti in domiselnosti nepridipravov na koncu pripelje do okužbe in sramotnega obnavljanja zadnje varnostne kopije diska. Zategadelj to priložnost izkoristite za preverbo še tako debelih ščitov.

Virusna nadloga

Prvi korak pri snovanju uspešne obrambe je poznavanje nevarnosti. Enostaven seznam vseh lukenj žal ne obstaja, kajti splet je dinamično, hitro razvijajoče se okolje, kjer se vsak dan rodi kaj novega. To še kako drži za zlobno kodo (s tujko malware ali malicious software) – za njo stoječe glavce si nenehno izmišljujejo sveže načine za zaobitje zaščit. Tako je predvsem na vas, da sledite trendom in redno spremljate novice s področja spletne varnosti. Odličen tovrstni pripomoček so RSS-viri varnostnih podjetij, denimo F-Secure in Kaspersky. Z njih prebiranjem boste domala instantno obveščeni o vsem potencialno nevarnem dogajanju.

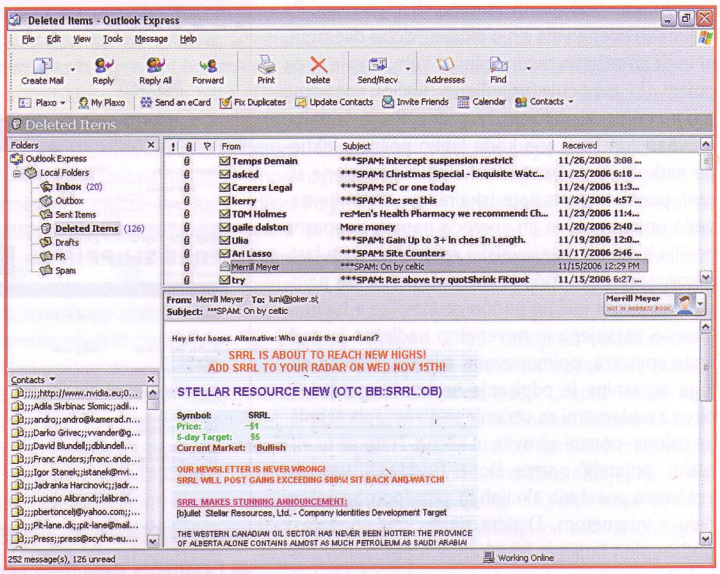
Katere pa so najpogostejše oblike zlobe kode? Prvo omembo si zaslužijo dobri stari virusi. Čeravno ti nepridipravski programčki v najosnovnejši obliki počasi izginjajo, so zgled in razvojni model za vse moderne šampione zlobe. Virusi so skupki kode, ki so privzeto nemočni in nenevarni. Aktivirajo se šele, ko po zgledu svojih bioloških soimenjakov napadejo drug program – žrtev okužijo oziroma njeno kodo umažejo s svojo. Osnovna naloga virusov je širjenje. Najprej dobra onečastijo domače računalo, kjer se razpasejo po kar se da velikem številu aplikacij. Ko okužen softver skopirate kolegu, se virus razmnoži še po njego-

vem kompu. In tako dalje. Ne preseneča, da so bile njega dni glavno leglo zlobne kode univerze. Ruljeki so tamkaj uporabljali relativno majhno število prosto dostopnih računalnikov in kot za stavo menjavali pisalno nezaščitene diskete.

S prebojem cedejev, ki ne omogočajo tako preprostega spreminjanja zapisane vsebine, je moč klasičnih virusov pričela pešati. Število različic in okužb je upadlo do te mere, da se je začelo govoriti o koncu dobe virusov in predsednikom varnostnih podjetij so po vrsti začeli izpadati lasje. A potem se je zgodil širokopasovni internet in virusi so znova dobili sanjski medij za razmnoževanje. Nadvse so jim pri srcu nenadzorovani P2P-izmenjevalni programi. Presenečni bi bili nad številom naivnežev, ki ne preverijo z Mule ali kakega drugega servisa potegnjenega filetka, temveč ga kojci zaženejo, v dobri veri, da gre za želeno igro ali film. Še učinkovitejši so e-poštni virusi, kot sta Melissa in ILOVEYOU. Dotični igrajo na isto karto kot ostale podvrste: zanašajo se na naivnega človečka, ki mora lastnoročno pognati e-pošti priloženo priponko. Po okužbi je virusova prva naloga, da se razpošlje na

Mutacije zlokode

Kljub temu je zadnje čase najpogosteje v središču pozornosti alternativna oblika malwara, in sicer črvi. Gre za evolucijsko obliko virusov, ki je drugotno namembnost v večji meri podredila prvi. Črvi izkoriščajo varnostne luknje v operacijskih sistemih in aplikacijah za širjenje brez človeškega posredovanja. Zategadelj se množijo docela samodejno in z možgane kravžljajočo hitrostjo. Neslavni Code Red se je v prvih devetih urah obstoja



V čisto vsaki od priponči na sliki se skriva zlokoda. Nje avtorji se zanašajo na to, da jo bodo nevedni uporabniki odprli in zagnali. Nemara bi si mislili, da takih naivnežev ni veliko, a hitrost širjenja e-poštnih virusov pravi drugače. Naj na limanice ne dobijo tudi vas!

Če je brskalnik nepravilno nastavljen, vas lahko okuži že vstop na take strani. Zato si ubodite Firefoxa ali Opero.

vse naslove v žrtvinem adresarju, s čimer doseže blazno hitrost širjenja. Med pohajkovanjem Melisse je moralo nekaj velikih podjetij kratkomalo izklopiti svoje e-poštne strežnike!

Drugo poslanstvo virusov je hkrati razlog, zakaj so tako nezaželeni. Po izpolnitvi določenih pogojev, recimo števila okuženih aplikacij ali preddoločene ure na za avtorja pomemben datum, se virus aktivira in okuženca naposled opozori na svoj obstoj. Nekateri izpišejo le kako neumestno sporočilo tipa 'Luni pwnz j00 and ur s1ster!', določeni pa se zadovoljijo šele s sesutjem Oken ali celo izbrisom diska.

uspel razširiti na neverjetnih četrt milijona računalnikov, Mydoom in Slammer pa sta bila še uspešnejša. Tako naglo razmnoževanje ima posledice že samo po sebi. Ko črvi preverjajo okoliško mrežo, da bi našli tarče, v splet pošiljajo gromozanske količine paketkov. Število le-teh tako narasteta, da se osrednji usmerjevalniki znajdejo v težavah. Ko ruterji vsled črvoidnih paketov niso več sposobni pravočasno obdelovati legitimnih zahtevkov uporabnikov, to opazimo kot porast odzivnih časov, zmanjšanje prepustnosti ali celo popolno nedosegljivost servisov. Z drugimi besedami: črvi so med razmnoževanjem sposobni zasesti internet. A dosti se jih s tem ne zadovolji in s seboj nosi neprijetna presenečenja. Znani so primeri, ko je bil črvu pripet trojanec, rootkit, navodilo za DDOS-napad na spletno stran, ukaz za izklop računala ali kaka druga nevšečnost. Najbolj grozljiva lastnost črvov pa je, da jih praktično ni mogoče prestreči in onemogočiti. Edina zanesljiva obramba pred njimi sta dobra posodobljenost in zakrpanost vsega sistema.

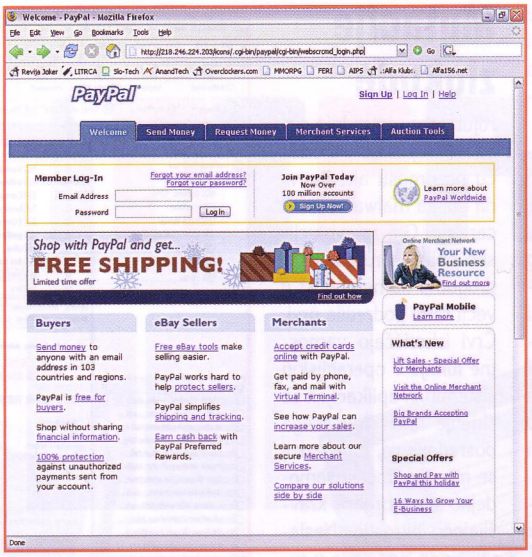
A celo črvi so nenadležni v primerjavi z naslednjo ve-

MOBIDIČNI VIRUSI

Virusi že dolgo niso več omejeni na računalnike. Prvi mobilniški malware so na Japonskem odkrili že dvatisočega, trenutno pa je v obtoku nad petsto črvov za tulifonične operacijske sisteme. To ni nič presenetljivega, kajti sodobni mobidiki postajajo vse podobnejši abakom – opremljeni so s hitrimi procesorji, velikimi količinami pomnilnika, grafičnimi vmesniki, zmožnostjo komuniciranja po več omrežjih ... Večina telefonskih virusov še ni posebej škodljivih, saj izpisujejo smešna sporočila, spreminjajo ikone ali malenkostno otežujejo rabo določenih funkcij. A enako so začeli njihovi računalniški bratje, nakar so se iz njih razvile pošasti, ki so mnoge ljudi konkretno finančno oškodovale. Vse kaže, da je mobitelovski malware na podobni poti. V obstoju so primerki, ki tako sesujejo operacijski sistem telefona, da pomaga le obisk serviserja. Nemara še mnogo neprijetnejši pa so tisti, ki brez privolitve lastnikov kupijo petdeset zvonilnih melodij ali kličejo drage plačilske številke. Ravno s tako nadlogo se ubadajo v Rusiji. Še ena neprijetna lastnost mobidičnih virusov so mnoge poti širjenja. Določeni se po zgledu e-poštnih črvov prenašajo po SMSih, za nekatere je dovolj že odprta modrozoba povezava, kmalu pa je pričakovati prave epidemije po GPRSu ozirom UMTSu. Varnostna podjetja so se že odzvala; F-Secure recimo ponuja protivirusni paket za mobilnike z operacijskim sistemom Symbian.

liko skupino malwara: vohunino ali spywarom. Po nekaterih ocenah sta z njo okuženi dobri dve tretjini vseh omreženih računalnikov! Vohunina je širok pojem, ki označuje prihuljene, večini neopazne programčke, ki delujejo brez dovoljenja lastnika računalnika. Pretkana koda lahko počne praktično karkoli – preusmerja brskalnik na neželene strani, poneverja rezultate iskalnikov, spremlja navade uporabnika in jih sporoča naprej, neopazno pošilja klike na oglaševalska spletišča svojih lastnikov, spreminja modemske nastavitve, da namesto na Arnes kličete naddrage številke v tujini ... Posebej razširjena in neverjetno nadležna je podvrsta spywara, poimenovana adware. Glavna naloga oglasnine je odpiranje neskončnega števila oken z reklamami za večanje penisov, zobotehniške usluge, poceni zdravila in slično. Nato so tu virtualni 'prijatelji' pasme Bonzi Buddy, ki vas obveščajo o posebnih akcijah in vam 'pomagajo' pri delu z internetom. Dotični največkrat spadajo v podskupino browser hijackerjev, ugrabiteljev brskalnikov, saj se tako zažrejo v spletni brkljalnik, da ga skoraj docela predrugačijo in jih je povrhu skrajno težko v celoti odstraniti. Še ena nadležna lastnost vohunine je, da pogosto onemogoči vse zaščite računalnika in na ubogo mašino privabi trumo zlobnih prijateljčkov. Je pa res, da z njo okuženih strojev ni težko prepoznati. Če že umanjkajo okna z reklamami, je dober pokazatelj petminutno zaganjanje Worda na sicer spodobni mašini. Vse to silno programje, ki laufa v ozadju, pač odžira nemalo pomnilniškega prostora in procesorske moči.

In kako se spyware širi? Dobra novica je, da samodejnega razmnoževanja ni zmožen, razen če brskalnik nastavite na najnižjo varnostno raven in surfate po piratskih ter porno straneh. Slaba pa je, da ga je moč najti v alarmantno širokem naboru sumljivih programčkov ter dodatkov. Nepridipravska koda se lahko skriva kjerkoli, od vtičnikov za brskalnike prek programov za P2P (po tej plati neslavna sta Edonkey ter Kazaa) do orodij za virtualne pogone. Posebej nesramen in žal učinkovit način širjenja so lažni antispyware programi. Najbrž ste opazili reklame, ki vas prepričujejo, da je vaše računalo okuženo z vohunino in da naj si dolpotegnite ter namestite aplikacijo, ki jo bo očistila. Dotični progiji vam znajo mlinček tako zabasati z malwarom, da vam ne bo mogel pomagati niti protivirusni bog.



Legitimna Paypalova vstopna stran? Naka, phisherska past, ki bo izvabila vaše osebne podatke in vas okradla!

Ste mislili, da je konec? Kje pa. Zlobni možgančki so pridelali za poln vagon drugih nevarnosti. Med hujše spadajo trojanci oziroma trojanski konji. Gre za progije, ki se pretvarjajo, da so legitimna aplikacija, igra, film, empetri filetek ali praktično karkorli drugega, a so v resnici zlobna koda. Trojanci so po učinku blizu klasičnim virusom, saj s svojo tarčo radi počno neizrekljivosti, kot je brisanje zagonskega dela diska. Nato so tu prej omenjeni rootkiti. Čeprav še ne uživajo tolikšne (ne)slave kot druge oblike malwara, bodo rootkiti v prihodnosti predstavljali eno največjih težav. Njihova edina naloga je prikrivanje dejavnosti druge zlobne kode. Z rootkitom ozaljšane vohunine sploh ne boste opazili v upravitelju procesov, raziskovalec njenih filetkov ne bo prikazal, okenski search je ne bo našel, večidel nemočni so celo antivirusniki. Rootkiti so zato idealni pajdaši ostalih elektronskih barabinov in le upamo lahko, da bodo varnostna podjetja iznašla učinkovite načine za njih detekcijo ter onemogočitev. Med zanimivejše nadalje spada družina ransomware. Ta podoblika vohunine je zelo agresivna in uporablja hudičevo domiseln način za sesanje denarja nesrečnim žrtvam. Ob aktivaciji preišče disk za tipičnimi oblikami datotek (posebej ji teknejo Wordovi in Excelovi fileti), jih stisne v zaščiteni arhiv ter pusti navodila za plačilo odkupnine. Ko avtorju

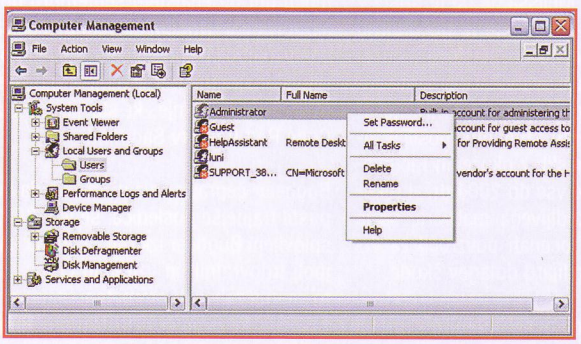
nakažete denar, dobite geslo za povrnitev dragocenih datotek, v nasprotnem primeru pa vas čaka mukotrpno in dolgotrajno delo s programi za obnovitev podatkov na disku. Ker ransomware krši mnoge zakone, na srečo ni tako razširjen, toda v porastu je njega druga generacija, ki žrtve sili v nakup sumljivih zdravil iz kake indijske spletne trgovine.

No, bržda najbolj nevarna in neprijetna oblika internetne nevarnosti je phishing (pri nas mu rečejo ribarjenje gesel). To početje spada med goljufije in ne zlobno kodo, a vsled uspešnega sodelovanja s slednjo si zasluži obdelavo v istem kontekstu. Phishing pomeni poneverjanje znanih strani z namenom kraje osebnih gesel, številk bančnih ter kreditnih kartic in drugih občutljivih podatkov. Nepridipravi v ta namen ustvarijo skorajda popolno kopijo Amazona, Ebaya, Paypala, vstopnega portala za elektronsko bančništvo ali kakega drugega priljubljenega spletišča, le da polja za vpis podatkov vodijo na njihove strežnike. Ko nič hudega sluteč uporabnik vtipka svoje ime in geslo, ju pošlje neposredno zlobnežem! Prve phisherske strani je bilo moč zlahka prepoznati po slovničnih napakah in nedelujočih sličicah, današnje so pak neprimerno naprednejše. Vsebino servirajo neposredno s strežnikov originalne strani, edino skripte za vpis vodijo v njihove baze. Pagine zato praktično ni mogoče razločiti od prave. Glavna težava phisherjev je pripraviti žrtve do obiska njihovih pasti. Pri tem se najpogosteje poslužujejo lažne e-pošte, ki jo spišejo v imenu upravitelja pravega spletišča. V njej trdijo, da je prišlo do napake, sesutja strežnikov, zatika v obdelavi podatkov ali česarkoli pač in da morate posodobiti uporabniški račun. V pošti priložena povezava nato kakopak vodi do ribolovske strani. Ker se je rulj navadil na tovrstne poskuse in začel ročno vpisovati naslove kritičnih strani oziroma nucati direktne brskalnikove zaznamke, so se ribolovci povezali s snovalci vohunine. Ta po novem spremeni vaš brskalnik tako, da vas ob vpisu recimo *www.amazon.com* samodejno in neopazno preusmeri na phishersko past. Pri tako dodelani in nevarni goljufiji vam ne preostane drugega kot redno zaganjanje antivirusnikov in antispajverovskih aplikacij.

Gradnja bunkerja

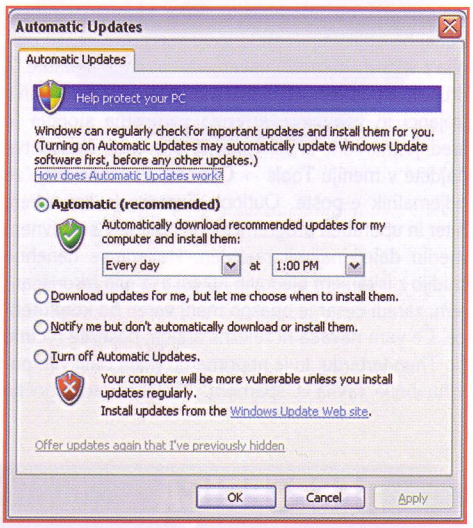
Kot sem omenil v uvodu, popolne, neprebojne zaščite proti vsem internetnim nevarnostim ni. Stoodstotno zavarovan abak je le tisti, ki je fizično odklopljen s spleta in na katerega nikoli ne nameščate novega programja. Če lahko krekerji vdrejo v bančne strežnike in Pentagonove stroje, ste lahko prepričani, da jim vaš domači strojček ne predstavlja nobenih težav. Vprašanje je torej, kako zagotoviti 99,9-odstotno zaščitenost, kar je tudi za neznalca realen cilj.

Na prvem mestu je izbira operacijskega sistema. V Microsoftovem naboru so kolikor-toliko primerna le Okna 2000, XP in 2003. Mnogi bi na tem mestu priporočali uporabo Linuxa, a čeravno je ta privzeto neprimerno manj luknjast od XPjev in zmore biti spodobna osnova za vsakodnevno neigrarsko računalo, ostaja eksotika za znalce. Ogromna večina vas bo vsaj do prihodnjega leta, ko pride Vista, ostala na Ikspejih, zato poglejmo, kaj je moč storiti z njimi. Prvi korak bi morali storiti že med inštalacijo, in sicer izbrati primerno geslo za osnovni administratorski uporabniški račun. Mnogim lenuhom se med zaganjanjem računala ne ljubi porabiti tistih štirih sekund za vpis gesla, zato račun pustijo brez šifre. S tem pa ubijejo vse nadaljnje zaščite, kajti prost dostop do upraviteljskega računa so mokre sanje vsakega hekerja. Zato izberite primerno kompliciran geslo in račun iz očitnega 'Administrator' preimenujte v nekaj drugega, recimo 'Chokolino'. To storite tako, da v nadzorni plošči poiščete Administrative Tools, poklikate ikono Computer Management, v drevesnem meniju dobljenega okna izberete Local Users and Groups in v mapi Users poiščete Administrator. Z desnim klikom prikličete meni, v katerem je možnost Rename. V isti sapi onemogočite račun za goste, ki je prehod za nekaj znanih zlorab. Izbrisati ga žal ne morete, tako da v desnoknofovskem meniju izberite Properties in obkljukajte kvadratek pri možnosti 'Account is disabled'. Poslej bo v seznamu ob sličici rdeči križ, ki označuje nedejavnost. Zelo dobra izbira je takisto stvaritev posebnega računa za vsakodnevno rabo, ki mu omejite pravice na minimum. S tem preverjeno onemogočite dobršen del vohunine, virusov in trojancev, ki se zanašajo na polne sistemske pravice. Druga stran kovanca je dejstvo, da boste morali pri inštalaciji vsakega novega programa, da ne govorim o gonilnikih, preklapljati na upraviteljski account. Komur se s takimi malenkostmi ne ljubi ukvarjati, lahko poskusi namenske programčke za omejevanje pravic. Eden priročnejših je 1-Defender, ki omogoča stvarjenje posebnega namizja z bližnjicami do programov, ki se zaganjajo brez administrativnih privilegijev. Nekaj podobnega počne DropMyRights, ki ga je pred leti spisal eden od Microsoftovih strokovnjakov za varnost.



Upraviteljski račun nikoli ne sme biti brez gesla! Takisto se splača izklopiti dostop za goste, saj se skozenj šunja malware.

Druga možnost je totalna ločitev brskalnika od preostanka sistema. Microsoft kani v Visti udejanjiti prav to, zaenkrat pa so rešitev namenski progiji a la Greenborder Pro in Virtual Sandbox, ki odrežejo vse povezave med brskalnikom ter operacijskim sistemom. Četudi kaki vohunini uspe priti skozi, se ne more ugnezditi v sistemski del registra ali pisati na disk. Poglavitni težavi virtualizacijskega softvera sta cena in nepraktičnost. Virtual Sandbox recimo nenehno gnjavi z opozorili o nevarnosti in zahteva potrditev za vsako malenkost. Še bolj preganjavični bodo posegli po zastonjskem, a zajetnem paketu, ki ga je izgotovil VMWare. Znani razvijalec virtualizacijske tehnologije je pripravil navidezni operacijski sistem, osnovan na Ubuntu, eni od inačic Linuxa. Okolje lepo deluje pod Okni in vsebuje le Firefox. Zlobna koda, ki se šunja skozi brskalnik, tako namesto na ranljive Winse naleti na robustno linuksaško okolje, kjer večinoma žalostno odmre. Če se v Firefox naselijo razni nezaželeni dodatki in ugrabitelji, pa softver omogoča preprost reset na privzete nastavitve.



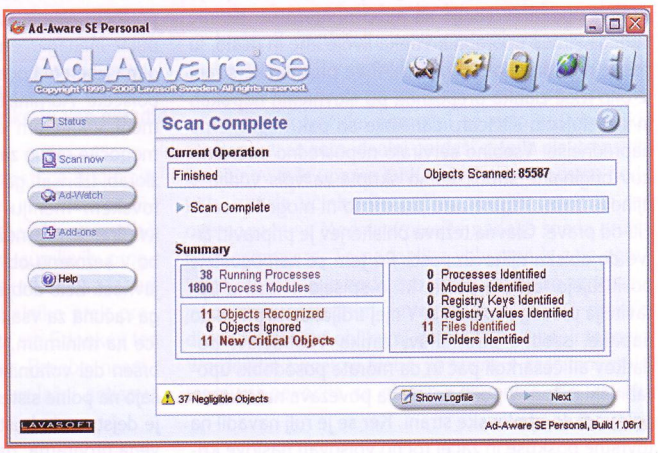
Automatic updates niso nikakršen bavbav, vreden izklapljanja. Pustite jih pri miru in nemalo črvoidne zalege bo onemogočene.

Naslednja pomembna navada pri zagotavljanju varnega delovnega okolja je omogočenje samodejnih posodobitev za Okna. Iz sila nedoumljivega razloga marsikdo izklopi avtomatski zaplatnik, češ da gre za brezvezno Microsoftovo orodje za krajo osebnih podatkov. Kar je približno enako, kot bi svoj avto zakurblan in odprtih vrat ponoči pustili sredi velemesta ter menili, da bo vse kul, saj so varnostniki na parkiriščih itak barabe. Žalostno dejstvo je namreč, da ima na internet priklopljen, nezaflikan in nezaščiten stroj povprečno življenjsko dobo okoli 27 minut. To pomeni, da bo po vklopu običajno v manj kot tridesetih minutah posiljen, onečaščen in prepreden s črvi. Av-

tomatske posodobitve so pomembno varnostno orodje in v veliki meri onemogočajo črve. Da je tako, sem se ničkolikokrat prepričal na lastni koži. Ko je pred leti razgrajal Blaster, ki je nenadzorovano izklapljal računalnik, sem za njega izvedel šele skozi novice, ducat znancev pa ni bilo tako srečnih. Skupna točka vseh? Izklopljeni Automatic updates ...
Veliko vlogo takisto igra izbira aplikacij za delo s spletom. Internet Explorer 6 je s stališča varnosti skoraj neverjetno zanič. Polno posodobljen in zakrpan se je sicer zmožen dostojno upirati zlobni navlaki, a preden vam to uspe, boste po vsej verjetnosti že fasali kakega nepridiprava. Zato bi moral biti prvi korak po namestitvi novega operacijskega sistema vtipk naslova *www.firefox.com* ali *www.opera.com* in dolpoteg vsaj nekoliko varnega brskala. Tej dvojici se je nedavno pridružil Internet Explorer 7, ki je velik korak naprej od predhodnika. (Glej primerjavo brskalnikov v prejšnjem Jokerju.) A Lisica in Opera še vedno delujeta robustneje in bolje ravnata z nadležnimi pojavnimi okni, ki dostikrat nosijo vohunino. Še en pomemben napotek glede brskalnika: nikoli, ampak res NIKOLI ne uporabljajte nizke stopnje varnosti! Tedaj bo aplikacija veselo jedla vse piškotke, se polnila z vtičniki in brez vprašanja nameščala dodatke. Z drugimi besedami, računalnik bo v četrt ure naphan s trojanci in vohunino. Privzeta varnostna stopnja je srednja; naredite si uslugo in to preverite. Nastavitve najdete v meniju Tools -> Options. Podobno velja za odjemalnik e-pošte. Outlook Express je spodoben, hiter in uporaben programček, vendar je v svetovnem merilu daleč najbolj razširjen. Hekerji se nenehno trudijo z iskanjem njegovih lukenj in z njih izkoriščanjem, zaradi česar je opazno manj varen od konkurence. Če vam navada ni železna srajca, posezite recimo po Thunderbirdu, ki je neprimerno manj ranljiv in povrhu bolje ravna s spamom. Nadalje onemogočite branje pošte v formatu HTML in blokirajte prikazovanje sličic, ki niso priložene sporočilu (tako imenovane third-party images). Sicer še vedno ostanejo priponke z virusi, a boste vsaj onemogočili praktično ves samodejno nameščajoči se e-poštni malware.

Ne bodite naivni!

Nenazadnje k delu z internetom vedno pristopajte z zdravo mero dvoma. Naivnost in zaupljivost sta lastnosti, ki bi ju internauti morali pustiti za sabo. Kot je povedal eden od gurujev varnosti: 'Softver lahko zakrpaš, toda nihče še ni izumil zaplate za človeške možgane'. Če boste odpirali vsako e-poštno priponko, klikali vse povezave in si nameščali desetine sumljivih programčkov ter brskalniških dodatkov, vam ne bo pomagala še tako zaščitena mašina. Rezultati lepo kažejo, da je daleč najbolj uspešen tisti malware, ki uporabnika psihološko pretenta. Spomnite se virusa ILOVEYOU, ki je igral na človeško potrebo po ljubezni. V ZDA je bil skorajda enako uspešen email-virus, ki je ljudi prepričeval, da so toženi in da se lahko rešijo le, če odprejo priponko. Kot veste, se Čezlužci manično bojijo tožb ... Zato se navadite, da sploh ne prebirate mailov od neznanih, očitno tujih oseb, kaj šele, da bi odpirali priložene datoteke. Še več, ne zaupajte niti vsem sporočilom od znancev, saj se ogromno malwara razpošilja ravno skozi dejanske adresarje. Slovenci smo tu v prednosti, kajti avtomatsko zgenerirana virusna sporočila so ponavadi v angleščini, ki je ne gre ravno pričakovati od strica ali soseda Rudija. A kot kažejo aktualni ribarski napadi na elektronsko bančništvo NLB Klik in strani za prijavo v Siolov sistem, je tudi pri nas dovolj posameznikov, ki se jim ljubi producirati malware. Le vprašanje časa je, kdaj bomo fasali zlobno kodo v slovenščini.
Enaka mera opreznosti velja za brskanje. O obiskovanju le znanih in preverjenih spletišč vam ne nameravam predavati, vsakdo kdaj zaide na kako pornjaško stran ali zbirko krekov. Toda če že brskate po takšnih okoljih, se vzdržite klikanja na povezave, oglase in predvsem popupe. Ne zapirajte jih s klikom na gumb 'No', 'Cancel', 'No, thanks!' in podobno, saj se pod njimi pogosto skriva ravno obratna funkcija. Nadlogo terminirajte s stiskom tipk alt + F4. Glede nepreverjenih pluginov in dodatkov bi vam že vse mo-



Spyware ali vohunina sega od relativno nenevarnih brskalniških piškotkov do malicioznih aplikacij, ki žrtev okradejo.

DESETERICA NAJZLOBNEJŠIH

Virusi so neločljiv del računalniške zgodovine, zato ni čudno, da je prve omembe o njih moč najti že v zgodnjih osemdesetih. Starejši bralci se najbrž spominjate Jerusalema, Michelangela, Tequile, Chernobyla, Word Concepta in ostalih slavnih zlokodnežev, ki so grenili naša življenja v ranih dneh modernega računalništva. A celovito gledano so bili ti virusčiči pravi amaterji proti nakazam, ki so harale pozneje in so povzročile alarmantne količine škode. Tukaj je izbor deseterice najodmevnejših.

Melissa: prvi pravi e-poštni virus je za sabo pustil pravo razdejanje. Širil se je skozi priponke, ki so vsebovale okužen Wordov dokument. Po odprtju se je Melissa instantno razposlala na prvih petdeset naslovnikov v žrtvinem adresarju. S hitrostjo množenja je povzročila pravo paniko, mnogo korporacij, vključno z Microsoftom, je bilo primoranih izklopiti svoje e-poštne strežnike. Melissa je okužila okoli milijon računalnikov in povzročila za okrog 80 milijonov dolarjev škode, njen avtor pa je pristal v zaporu za dvajset mesecev.

ILOVEYOU: strah pred milenijskim hroščem in napovedi o koncu sveta je spomladi dvajurjevega še podžgal e-poštni virus ILOVEYOU. Deloval je podobno kot Melissa, le da je prišel v obliki filetka .vbs in se je po odprtju razposlal na čisto vse naslove v adresarju. Povrhu je vseboval elemente vohunine, saj je svojemu avtorju, nekemu filipinskemu študentu, pošiljal informacije o geslih z okuženih računalnikov. Love je vse do 2004 držal rekord najbolj škodljivega malwara, sa je po nekaterih ocenah povzročil za vrtoglavih 10 milijard dolarjev škode.

Bubbleboy: čeravno mehurnik ni bil preveč agresiven ali škodoželjen, je napovedal prihodnost zlobne kode. Velja namreč za prvega črva, torej virus, ki se ne zanaša na stupidno žrtev in njeno odprtje okužene datoteke. Širil se je potom dokumentov Offica.

Code Red: ta neslavnež je izviral iz Kitajske in se je širil z dotlej nevideno hitrostjo. V dvanajstih urah je padlo skoraj 360 tisoč spletnih strežnikov, opremljenih z Microsoftovim ranljivim Internet Information Services. Sprogramiran je bil tako, da bi na določen datum vse okužene računalnike uporabil za DDOS-napad na server Bele hiše, toda upravitelji so to odkrili in po hitrem postopku spremenili IP.

Nimda: da je bilo 2001. leto črvov, je teden dni po enajstem septembru dokazal Nimda. Dotični še vedno velja za enega najbolj izpopolnjenih, saj je uporabljal najmanj pet načinov okužbe, med drugim luknje, ki sta jih pustila Code Red II in črv Sadmind.

Bugbear: čeprav sprva ni kazalo, da bo pustil trajnejše posledice, se je v 2002 splovljeni Bugbear izkazal za enega najbolj trdovratnih in vztrajnih črvov. Za to se ima zahvaliti premeteni, napredni zasnovi, ki zasenči celo Nimdo. Bugbear je veliko gorja povzročil šele v naslednjih letih, predvsem 2003. V mutirani obliki je Bugbear.B ubijal procese več znanih protivirusnih in protipožarnih programov ter tako računala puščal ranljiva.

Slammer: januarja 2003 je Slammer najavil bogato leto za črve. Sam po sebi je bil dokaj neškodljiv, a je rušil rekord v hirosti širjenja: v desetih minutah po zagonu je okužil 75.000 računalnikov, nakar je število žrtev podvojil približno vsakih osem in pol sekund! Posledično je klecnil dobršen del spleta, škode pa raje sploh niso merili.

Blaster: par mesecev za Slammerjem je uletel Blaster. Zavoljo ranljivosti v RPC DCOM je prodrl v več različic Oken in delal štalo. Najbolj moteči učinek Blasterja, stalno resetiranje okuženega kompa, je dejansko posledica napake v izvorni kodi. Manj kot teden za Blasterjem je prišla Welchia, prvi koristni črv. Skušal je odstraniti Blasterja in popraviti luknjo v Oknih.

Mydoom: Mydoom oziroma Novarg še vedno drži rekord najhitreje širečega se črva. Zasnovno je podoben Sobigu, saj žrtve uporablja kot točke za posredovanje desetin tisočev okuženih sporočil. Glavna namembnost Mydooma je bil DDOS-napad na strežnike podjetja SCO Group, ki je takrat tožilo več odprtkodnih projektov. SCO je ponudil četrtmilijonsko nagrado za informacijo, ki bi pripeljala do prijetja avtorjev.

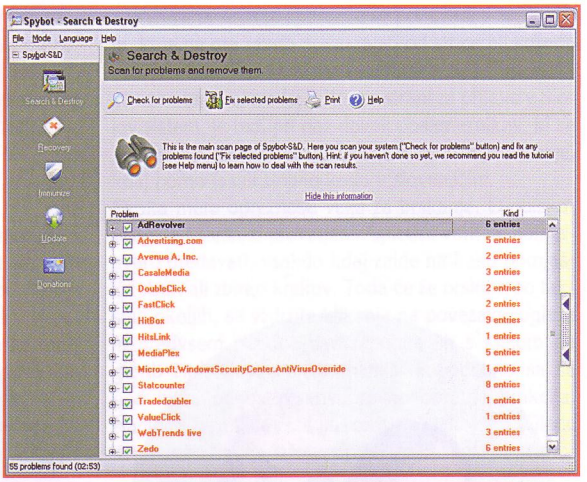
Sasser: črvoidni virus, ki ga je spisal 18-letni Nemec, je združil učinke Slammerja in Blasterja. Uspešno je okužil nepregledne množice računalnikov, med drugim dobro zaščitene delovne postaje bank, letališč in drugih podjetij. Upraviteljem je ogromno glavobolov povzročila njegova nagnjenost k naključnemu in nenehnemu resetiranju prizadetih strojev.

ralo biti jasno. Za uspešno brskanje potrebujete le Flash, javo in morda Shockwave. Vsi ostali vtiči so navlaka in predstavljajo tveganje okužbe, pa če so še tako opično prisrčni. Ako je bil avtor strani tako len, da svojega izdelka ni mogel zasnovati po široko sprejetih standardih, odsurfajte drugam. Izbire na spletu res ne manjka. Takisto se sledite povezavam na strani z overjenjem / avtentikacijo. Naslov zmerom vtipkajte ročno ali uporabite brskalniški zaznamek. O rabi kreditne kartice pa sploh ne premišljajte, če se v spodnjem desnem kotu brskalnika ne sveti ključavnica!

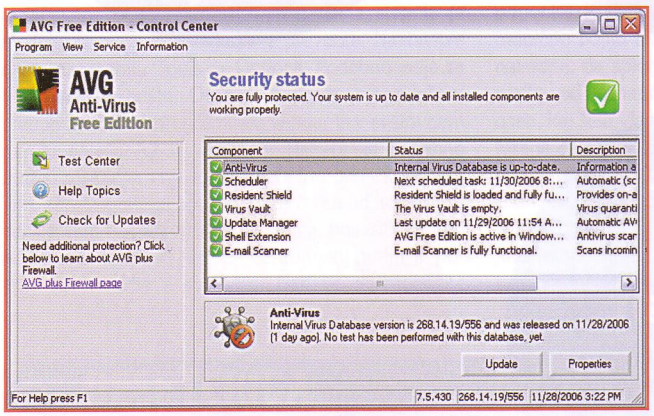
Vitezi na belih konjih

Kar se dejanske zaščite računala tiče, je prva linija obrambe vedno dober požarni zid, firewall. Razmislite o vložku v strojnega oziroma sodoben usmerjevalnik, saj ti zidove že vsebujejo. Strojni firewalli so preklemano učinkovita prepreka, posebej taki, ki podpirajo NAT (Network Address Translation), blokiranje in skrivanje portov, tehnologijo SPI (Stateful Packet Inspection) ter navidezne zasebne mreže oziroma VPN. Zlasti zanimiv je SPI, saj v veliki meri onemogoča črve, ki se zamaskirajo v obliko legalnega internetnega prometa, denimo e-pošte. SPI nadzoruje odhajajoče paketke in nazaj v računalo spušča le tiste, ki so odgovor na odposlane. Če se vam deset jurjev za ruter zdi pretiran izdatek, posezite po kakovostnem softverskem firewallu. Priloženi v Oknih XP je dovolj le za prve minute povezave v splet, preden dobite nekaj zmogljivejšega. Njegova največja težava je, da uravnava le promet v smeri k računalniku, medtem ko izhodnega ne. Če je sistem že okužen s kakim beležnikom tipk (keyloggerjem) ali vohunino, tej nič ne preprečuje prostega prometa z vašimi podatki. Komercialnih in zastonjskih firewallov je cel kup, zato je izbira vaša. Vsekakor se odločite za takega, ki omogoča blokiranje posameznih aplikacij. Za zanesljivega se je denimo izkazal dobri stari ZoneAlarm, nakar sta tu Kerio in moj favorit Tiny Personall Firewall oziroma po novem CA Personal Firewall 2007. Slednji ni tako uporabniško prijazen kot domala kičasti Zonealarm, vendar je izdatno prilagodljiv ter nastavljiv. Škoda le, da velja trideset dolarjev. Takisto priporočam, da sposobnost zidu preverite na kaki namenski strani. Najbolj znana je GRCjeva ShieldsUp!, ki jo najdete na *www.grc.com*.

Naslednji naj bo dober protivirusnik. Izbire ne manjka niti na tem področju – po spletu se svaljkajo desetine antivirusnih aplikacij, od zastonjskih do takih, ki so del dragih kompletov. Vsaka od njih je neprimerno boljša od popolnega manka zaščite, dočim je razlike precej težko najti. Z drugimi besedami, ne obremenjujte se s tuhtanjem o tem, kateri je boljši. Vsi veliki igralci skrbijo za redna samodejna posodabljanja virusnih baz, obvladajo sprotno preverjanje e-pošte in druge pomembne stvari. Razlikujejo se kvečjemu v hitrosti skreniranja, ki pa je itak pri vseh grozovito počasno (za popoln prečes diskovja in registra si rezervirajte kake pol urice). Ta hip so najboljši Bitdefender, Kaspersky in NOD32, zgrešili pa ne boste niti s starostami tipa McAfee Virusscan, F-Secure ter Norton. Takisto je pester nabor zastonjskih inačic. Od njih ne pričakujte ogromno, saj so manj zmogljive od plačljivih, tako pri zaznavanju kot hitrosti. Toda precej celoviti Antivir Personal Edition, Avast Home Edition in AVG Free Edition bodo nedvomno zadovoljili večino uporabnikov. Tako kot za požarne zidove za protivirusnike velja, da nikoli ne uporabljajte dveh ali več naenkrat, saj bo sistem postal še bolj neuporaben, kot če bi bil poln malwara. Preden zamenjate aplikacijo, trikrat poskrbite, da je stara odstranjena do poslednjega bita!



Redno česanje računala z Ad-aware in Spybotom je dober način obrambe proti vohunini.



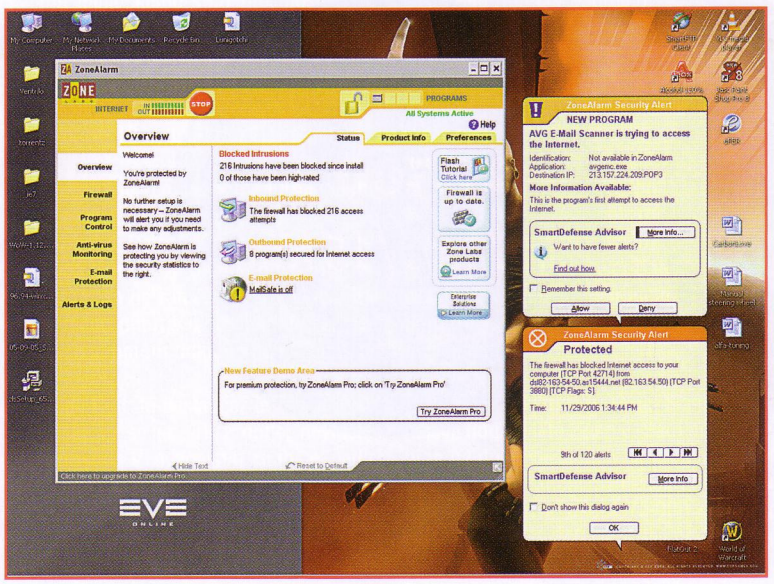
Antivirusnikov je dandanes na voljo cel kup. V večini primerov zadostujejo že najosnovnejše, zastonjske inačice.

Povsem nasprotno velja za antispajverovski softver, ki je zadnji v sveti trojici varnosti. Dotični progiji se ne ovirajo med seboj, prej nasprotno. Nobeden od njih ni zmožen zaznati in odstraniti čisto vse vohunine, tako da se pravzaprav odlično dopolnjujejo. Zato si le naložite fenomenalni Ad-aware, ga ozaljšajte s Spybot Search & Destroy ter oba zaokrožite s SpywareBlasterjem in SpywareGuardom, ki zlobni kodi onemogočata namestitev.

Kakopak obstaja še na stotine drugih programčkov, ki izboljšajo varnost računala. Priljubljeni so namenski blokirniki oglasov, recimo Webwasher Classic. Nekaterim se zdita upravičena inštalacija in raba nucnikov v slogu EULAlyzerja, ki preverijo pogodbo EULA (End User License Agreement – tista drobnotekstovna zadeva, ki jo morate potrditi pred inštalacijo vsakega programa) in iščejo postavke, ki dovoljujejo vohunjenje. Netcraft Toolbar in Earthlink Toolbar sta dodatka za brskalnike, ki razkrivata phishane strani. Sophos je izpljunil svoj zastonjski Anti-Rootkit, katerega namembnost bi morala biti jasna. Na *www.trojanscan.com* najdete nalinijski iskalnik trojancev. SpamBayes je le eden od desetin progijev, ki se borijo proti neželeni pošti. In tako naprej in tako naprej. A vse to so le pike na ijih oziroma jeklene konice na debelem zidu solidne obrambe. Preizkusite jih, če se vam ljubi ali ste malce paranoični, vendar boste z ustrezno konfiguriranim sistemom ter pravimi navadami varni tudi brez njih.

Pamet v roke!

Četudi ste se (in upam, da ste se!) prebili skozi ves članek, ste se dotaknili le površja vprašanja internetne varnosti. Gre za resno temo, s katero se vsak dan ukvarjajo tisoči strokovnjakov. Tako pri varnostnih podjetjih kot v mračnih sobanah, kjer avtorji virusov kujejo vražjo kodo. Del cene razvoja je pač dejstvo, da nikoli ne bomo čisto varni in da za vsemi lepotami ter uporabnostjo interneta čepi njega temna stran. Zagata bo v prihodnosti postala še bolj pereča, kajti računalniške komunikacije prodirajo v vse pore našega življenja. Varni niso niti pametni telefoni, dlančniki in robidnice, kaj kmalu lahko pričakujemo napadalce na omrežene elektrozabavljaške pripravе, nemara bodo nekoč poslušnost odpovedali celo hladilniki in mikrovalovke. Prostor za zlobno kodo je povsod, kjer domujejo čipi s sposobnostjo povezovanja. Zato se ne prepustite brezskrbnosti: spremljajte novice, nadgrajujte obrambne okope in oljite mehanizme na virusnih pasteh!



Vdelani požarni zid v XPjih ne zadostuje! Računalu privoščite spodobno namensko aplikacijo, še bolje pa je, če kupite strojnega ali dober usmerjevalnik.