

ESET

Vsak računalnik je lahko orožje

..ŠTEVILO RAČUNALNIKOV, KI SO NA INTERNET PRIKLJUČENI BREZ PROTIVIRUSNE ZAŠČITE JE ŠE VEDNO OGOROMNO. TAKŠNI RAČUNALNIKI SO ZA KIBERKRIMINALCE IZVRSTNO SREDSTVO ZA DOBER ZASLUŽEK..



Občasno tudi pri nas še vedno srečamo uporabnike, ki so prepričani, da protivirusnega programa na svojem računalniku ne potrebujejo. Svoje prepričanje navadno spremenijo šele tedaj, ko je njihov računalnik okužen in upočasnjen do te mere, da je praktično neuporaben. Najpogostejši argument takšnih uporabnikov je ta, da na svojem računalniku tako nimajo podatkov, ki bi bili karkoli vredni. Dejstvo je, da lahko kiberkriminalci takšne računalnike s pridom izrabljajo in z njimi dobro služijo. Vključijo jih lahko v omrežje z ostalimi okuženimi računalniki (botnet) in izkoriščajo za pošiljanje neželene elektronske pošte, napade na spletne strani in ostale računalnike, nameščanje nevarnih programov ter za hrambo in širjenje nelegalne programske opreme in vsebin, ki lahko neodgovornega uporabnika spravijo v velike težave. Na takšnih računalnikih se lahko recimo znajde tudi otroška pornografska vsebina, oblastem pa je vse prej kot preprosto dokaza-

ti, da se na računalniku nahaja brez vednosti lastnika računalnika.

Vse pogostejša je tudi škodljiva koda, ki na okuženih računalnikih šifrira vsebino trdih diskov ali ukrade zgodovino obiskanih spletnih strani in jih objavi na spletu. Od lastnikov takšnih računalnikov kiberkriminalci potem v zameno za ključ, ki takšne podatke odšifrira, zahtevajo odkupnino. Zadnji takšen primer večjih dimenzij se je pred tedni zgodil ob izbruhu trojanskega konja Kenzero na Japonskem. Tisti, ki so izsiljevanju nasedli in so odkupnino plačali (ta je znašala 1500 jenov ali 12 evrov), so kiberkriminalcem posredovali podatke o svojih kreditnih karticah, njihovi dokumenti, slike in glasba so ostali šifrirani, njihova zgodovina obiskanih spletnih strani pa še vedno ostaja javno dostopna na spletu. Pisci trojanskega konja Kenzero imajo svoje prste vmes tudi pri zloglasnem črvu Koobface in omrežju okuženih računalnikov Zeus, zato ni dvoma, da gre za dobro organizirano kriminalno združbo. Zelo podobna grožnja se je pojavila tudi že v Evropi, v tem primeru pa avtorji trojanskega konja uporabniku okuženega računalnika grozijo zaradi domnevno nameščene nelegalne programske opreme. Pred takšnimi grožnjami se lahko zavarujete le z dobro protivirusno zaščito, ki mora biti



redno posodobljena, prav tako pa je pomembno tudi, da redno posodabljate svoj operacijski sistem in ostalo programsko opremo, ki je pogosta tarča izrabljanja varnostnih lukenj – to so spletni brskalniki, bralniki dokumentov PDF, predvajalniki multimedijskih vsebin itn. Prednost ESETovih varnostnih rešitev je predvsem v tem, da vključujejo napredno hevristično tehnologijo ThreatSense, ki je sposobna proaktivno prepoznati grožnje, ki jih ne zaznajo niti rešitve, ki temeljijo zgolj na pogostih posodobitvah zbirk virusnih definicij. ESET, v nasprotju s tradicionalnimi pristopi, izvršljivo kodo dekodira in analizira v emuliranem okolju, v resničnem času. Tako lahko ESETove rešitve škodljivo kodo prepoznajo takoj ob izbruhu. (P.R.)

eset
we protect your digital worlds

Varujemo vašo zasebnost

ESET SMART SECURITY

Antivirus
Antispyware
Firewall
Antispam

ESET NOD32 ANTIVIRUS

Antivirus
Antispyware

www.eset.si

SI SPLET, d.o.o. | Dolenjska c. 138, Ljubljana
01 428 94 05 | info@sisplet.com