

ESET

# Prevare z lažno protivirusno opremo

„SKOZI ZADNJI DVE LETI SPREMLJAMO VZTRAJNO NARAŠČANJE ŠTEVILA LAŽNIH PROTIVIRUSNIH PROGRAMOV, KI Z NAVIDEZNIMI REZULTATI PREISKOVANJ UPORABNIKE NAPELJUJEJO K NAKUPU NEOBSTOJEČE PROGRAMSKE OPREME.“



Vse do leta 2004 so na spletu prevladovala grožnje, ki so bile v veliki večini delo hobi programerjev ali računalniških zanesenjakov, tako imenovanih 'script kiddies'. Njihove grožnje v veliki večini primerov niso bile finančno motivirane. Po letu 2004 pa so se zadeve dodobra spremenile. Pisanja škodljivih kod so se namreč lotile tudi dobro organizirane kriminalne združbe, ki imajo v mislih en sam cilj, to je zaslužek. Poslušujejo se različnih metod, zadnji dve leti pa za prevare vse raje uporabljajo svoje lažne protivirusne programe, ki jih dejanski razvijalci protivirusne opreme uvrščajo med rouge grožnje oz. scareware. Cilj lažnih protivirusnih programov je uporabnika z izmišljenimi rezultati preiskovanj prestrašiti in ga napotiti na spletno stran, kjer lahko lažno protivirusno rešitev tudi kupi. Čeprav sam protivirusni program in njihova spletna stran v večini primerov izgledata povsem legitimno,

gre seveda za prevaro. Kiberkriminalci uporabnikom, ki takšnim prevaram nasedejo, prijazno ponudijo plačilo s kreditno kartico, poleg zaračunavanja neobstoječe protivirusne rešitve (cene takšnih 'programov' so različne, navadno se gibljejo okoli 50 evrov), pa tako pridejo tudi do podatkov, s katerimi lahko vašo kreditno kartico zlorabijo tudi na druge načine.

Grafični vmesniki takšnih programov so pogosto oblikovani tako, da spominjajo na resnične protivirusne rešitve, tudi imena datotek, ki naj bi jih program preiskoval, so resnična. Največkrat je uporabljen seznam z imeni sistemskih datotek operacijskega sistema Windows XP. Kiberkriminalci so iz računalnika, kjer je njihov program nameščen, sposobni prebrati tudi IP številko, zato lahko uporabniku na zaslon izpišejo tudi njegovo lokacijo, tako dajo uporabnikom se večji občutek kredibilnosti in zaupanja. Tudi spletne strani, ki ponujajo nakup takšne programske opreme, so oblikovane vrhunsko, zato ne čudijo ocene strokovnjakov, da je v zadnjem letu takšnim prevaram nasedlo približno 50 milijonov uporabnikov.

Pri zaznavanju in odstranjevanju takšnih nevarnosti je ključnega pomena proaktivna zaščita vaše protivirusne rešitve. Avtorji teh groženj svoje programe namreč nenehno spreminjajo in posodabljaajo, zato so protivirusni programi s

eset NOD32 TOP 10 <small>www.eset.si</small>	
Deset najbolj razširjenih groženj v zadnjem tednu	
	število okuženih e-sporočil
različica Win32/Injector.BZ trojan	14474
Win32/Zafi.B worm	10163
Win32/Netsky.Q worm	6280
različica Win32/Kryptik.YV trojan	1938
različica Win32/Kryptik.AZH trojan	1575
Win32/Netsky.Z worm	1446
Win32/Netsky.AB worm	1276
Win32/Netsky.C worm	1042
Win32/Mydoom.Q worm	389
različica Win32/Olmarik.PU trojan	232

klasičnim, reaktivnim pristopom, ki uporablja le virusne definicije, vedno korak za kiberkriminalci. ESETove protivirusne rešitve uporabljajo proaktivno tehnologijo ThreatSense, ki so jo razvili ESE-Tovi raziskovalci. Gre za najbolj napredno in izpopolnjeno proaktivno metodo na tržišču, ki škodljivo kodo prepozna v realnem času in ne šele po prenosu zbirke protivirusnih definicij. Tako se čas od izbruha takšnih groženj do ustrezne reakcije protivirusnega programa zmanjša na minimum. Tehnologija ThreatSense je uspešna, ker izvršljivo kodo pred dostopom dekodira in analizira v svojem varnem okolju in šele nato omogoči zagon. Vse to se zgodi v času, ki je za uporabnika neopazen, zagotavlja pa najvišjo možno stopnjo varnosti na spletu. (P.R.)

**NOVE CENE, PRILAGOJENE RECESIJI**

## Varujemo vašo zasebnost

**ESET SMART SECURITY**

Antivirus  
Antispyware  
Firewall  
Antispam

**ESET NOD32 ANTIVIRUS**

Antivirus  
Antispyware

[www.eset.si](http://www.eset.si)

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

**SI SPLET**  
INFORMACIJSKE TEHNOLOGIJE