

SPOROČILO ZA JAVNOST

Ljubljana, 16. 3. 2010

Evropo prizadel trojanski konji, ki pošilja neželjeno pošto

ESET-ov sistem za zbiranje podatkov o škodljivi kodi ThreatSense.Net je pokazal povečano aktivnost trojanskega konja Win32/Lethic.AA.

Kiberkriminalci lahko s tem trojanskim konjem upravljajo preko oddaljenega nadzora, izrabljajo pa ga za pošiljanje neželene pošte. Na računalnik se najverjetneje namesti skupaj z drugimi škodljivimi programi ali pa prenos sproži škodljiva koda, ki je pred tem na računalniku že nameščena. Glavni motiv avtorjev trojanskega konja je okužene računalnike povezati v omrežje z drugimi okuženimi računalniki (botnet), s pomočjo katerega bodo lahko pošiljali ogromne količine neželene e-pošte. Programsko kodo trojanskega konja so avtorji skrili v datoteko 'explorer.exe'.

Od sredine marca je Win32/Lethic.AA postal ena od najpogostejših globalnih groženj, najbolj pa je razširjen na Nizozemskem, kjer predstavlja že 13 odstotkov vseh groženj. Pogost je tudi v Estoniji (9%) in Belgiji (7%), v času nastanka članka pa predstavlja že 3 odstotke vseh groženj tudi na Danskem, Norveškem, Švedskem, Portugalskem in v Sloveniji. V kratkem času se je uvrstil tudi med dvajset najpogostejših groženj tudi na Slovaškem, Hrvaškem, Srbiji, Grčiji, Rusiji in Veliki Britaniji.

Za obrambo pred tem trojanskim konjem ESET priporoča nadgradnjo spletnih brskalnikov in protivirusnih rešitev ter večjo previdnost med brskanjem po spletu ter prenosu datotek.

Tehnologija ThreatSense.Net zbira anonimne statistične podatke o vrstah groženj na računalnikih svojih uporabnikov. Raziskovalci v ESET-ovem laboratoriju za analizo groženj imajo na podlagi teh podatkov natančen vpogled nad najbolj razširjenimi grožnjami v resničnem času. Škodljivi programi, ki jih prepozna ESET-ova hevristična zaznava so označeni posebej, zanje se pripravi posodobitev zbirke virusnih definicij, še preden se lahko razširijo ali mutirajo v druge različice.

O ESET

Podjetje je bil ustanovljeno leta 1992 in je že od samega nastanka usmerjeno v razvoj varnostnih rešitev. ESETovi produkti so že od vsega začetka ocenjeni kot eni od najboljših protivirusnih rešitev na trgu. Zaradi svoje tehnološke dovršenosti so bili že večkrat nagrajeni kot najučinkovitejši, najnatančnejši in najhitrejši protivirusni programi. Podjetje ima sedež v Bratislavi, svoje pisarne pa imajo še v Bristolu, Buenos Airesu, Pragi, San Diegu, s svojimi partnerji pa so prisotni v več kot 100 državah. Za več informacij obiščite www.eset.com ali pokličite +1 (619) 876-5400.

O SI SPLET

Podjetje se ukvarja s trženjem varnostnih in drugih rešitev na področju informacijskih tehnologij. V letu 2002 si je podjetje pridobilo ekskluzivno partnerstvo s podjetjem ESET za distribucijo varnostnih rešitev ESET v Sloveniji. Več na www.sisplet.com.