ESET

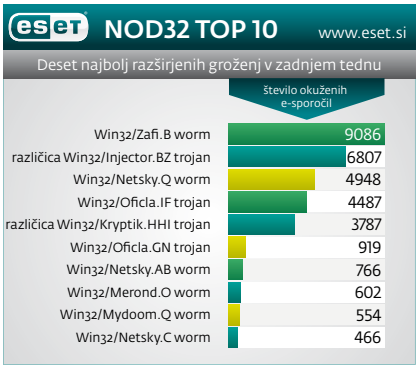
Najšibkejši člen smo uporabniki

..Poleg izrabljanja varnostnih lukenj v operacijskih sistemih in ostali programski opremi so v vzponu tudi škodljivi programi, ki se širijo s pomočjo socialnega inženiringa..

Po podatkih Mednarodne agencije za telekomunikacije (ITU) bo do konca leta na medmrežje povezanih že dve milijardi uporabnikov. Več kot šeststo milijonov nas bo aktivno sodelovalo v socialnih omrežjih kot so Facebook, Twitter in podobna, še veliko več uporabnikov pa se dnevno zadržuje na spletnih straneh, ki spadajo v tako imenovano sivo območje – to so spletne strani, ki ponujajo prenos nelegalne programske opreme in glasbe, pornografsko vsebino za odrasle in podobne. Te strani so pravilo-ma za okužbe najnevarnejše, saj obiskovalce pogosto preusmerjajo na druge nevarne spletne strani ali pa od njih zahtevajo prenos dodatnih kodekov za video vsebine ali ActiveX vtičnikov, ki so v resnici trojanski konji ali druga zlonamerna koda. Tudi uporabniki elektronske pošte smo dnevno bombardirani z lažnimi oz. ribarskimi sporočili, ki nam obljubljajo hiter zaslužek in poceni kupčijo. V vseh primerih gre za različne tehnike socialnega inženiringa, ki izrabljajo najšibkejši člen v verigi - uporabnika. Dejstvo je, da so kiberkriminalci pri socialnem inženiringu vse spretnejši – razvijajo vse bolj napredno programsko kodo, vse zvitejši so tudi pri tehnikah širjenja in vrstah prevar.

Upoštevajte nekaj nasvetov za večjo varnost:

Socialna omrežja temeljijo na modelu priljubljenosti – številčenje prijateljev, povezav ipd., vendar bodite previdni koga dodate med svoje prijatelje. Bodite nezaupljivi tudi do spletnih povezav, ki vam jih pošiljajo znanci - te vas lahko pripeljejo na spletne strani, ki vsebujejo škodljivo kodo. Veliko nevarnost predstavljajo tudi različni dodatki in spletne aplikacije za socialna omrežja. Te lahko zbirajo vaše osebne informacije, poleg tega pa so navadno precej ranljive, preko njih se lahko kiberkriminalci zlahka dokopljejo do vaših uporabniških podatkov. Priporočljivo je, da za obiskovanje spletnih strani socialnih omrežij uporabljate različne spletne brskalnike. Veliko manjša verjetnost je, da bodo kiberkriminalci zlorabljali varnostne luknje v brskalnikih, ki niso ravno standardni. Pogosta napaka je tudi ta, da uporabniki za dostop do različnih socialnih omrežij ter vseh ostalih spletnih storitev uporabljajo enaka uporabniška imena in gesla.



Kolikor je to le možno, se izogibajte spornim spletnim stranem, ki jih kiberkriminalci največkrat oglašujejo s pomočjo oglasov za razne popuste, brezplačno programsko opremo ali multimedijsko vsebino. Gre za obliko premetenega socialnega inženiringa, ki se ga moramo vsi uporabniki dobro zavedati. Programsko opremo prenašajte le iz uradnih spletnih strani.

Pri elektronski pošti bodite nezaupljivi do vseh sporočil, ki jih prejmete od neznanih pošiljateljev. Uporabljajte protivirusno programsko opremo, ki preišče priponke v sporočilih še preden jih prenesete ali odprete. Poskrbite tudi, da imate na svojem računalniku nameščeno zadnjo različico svoje varnostne rešitve, redno posodabljajte tudi svoj operacijski sistem, brskalnike ter vso ostalo programsko opremo. Nič manj pomembno ni, da je vaša protivirusna zaščita posodobljena z zadnjimi definicijami. ESETovi programi za zaščito pred škodljivo kodo poleg virusnih definicij uporabljajo tudi najnaprednejšo proaktivno zaščito na trgu, ThreatSense. Ta poskrbi, da ste varni tudi pred grožnjami takoj po izbruhu, saj škodljivo kodo analizira in prepozna v realnem času, tudi če grožnja med virusne definicije še ni dodana. (P.R.)