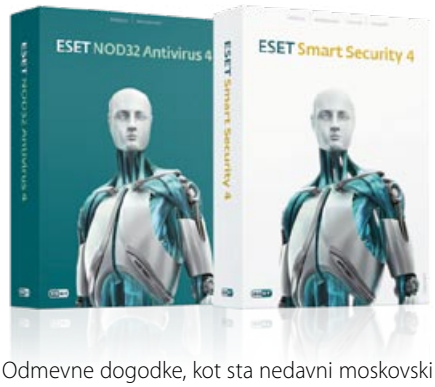
ESET

Kiberkriminalci že brcajo

..Junija letos se bo v Južnoafriški republiki začelo svetovno prvenstvo v nogometu. Pri ESETu so že zaznali prve resnejše grožnje, ki spektakel izkoriščajo za širjenje nevarne kode..



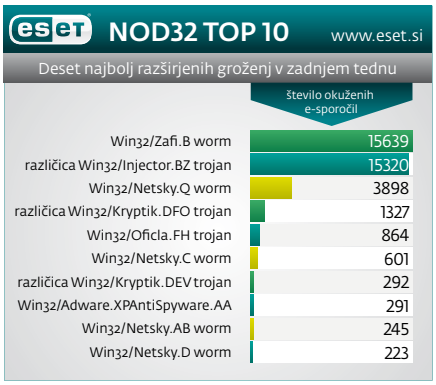
Odmevne dogodke, kot sta nedavni moskovski eksploziji v podzemni železnici in potres na Haitiju, kiberkriminalci za širjenje svojih programov izkoriščajo brez vsakega sramu. Nobena izjema ni svetovno nogometno prvenstvo, ki se prične v juniju. Pojavila se je že prva elektronska pošta, ki lahko računalnik (pre)radovednega uporabnika okuži s škodljivo programsko opremo. E-pošta v priponki vsebuje dokument PDF, ki izkorišča varnostno luknjo v programu Adobe Reader. To so pri Adobe sicer zakrpali 16. februarja letos, uporabnikov, ki programa od takrat še niso posodobili, pa verjetno ni malo.

Nevarno sporočilo na videz prihaja iz Južnoafriške turistične agencije Greenlife Africa, ki dejansko obstaja tudi v resnici. Besedilo sporočila je napisano v brezhibni angleščini, kiberkriminalci pa so v priponko pripeli kar originalen vodič turistične agencije, iz katerega so izbrisali nekaj strani besedila in v njega vključili svojo nevarno kodo. Potem ko uporabnik nevarno priponko odpre, se na njegovem računalniku ustvari in zažene nekaj datotek in namesti korenski komplet. Tako nameščena grožnja potem poskuša okužiti še ostale računalnike v omrežju.

Avtorji nevarnega sporočila najverjetneje izhajajo iz vzhodne Azije, ESETove protivirusne rešitve pa njihovo grožnjo prepoznajo pod imenom PDF/Exploit.CVE-2010-0188. Brez dvoma gre za dobro organizirano kriminalno združbo, ki jo bo težko izslediti.

Na srečo ne moremo isto trditi za hekerja, znanega pod vzdevkom SoupNazi, ki mu je ameriško tožilstvo konec prejšnjega meseca naložilo dvajsetletno zaporno kazen zaradi oškodovanja podjetij, bank in zavarovalnic za skoraj dvesto milijonov dolarjev. Čeprav je priznal, da je ukradel skoraj 135 milijonov številk kreditnih in debetnih kartic, je ameriško pravosodje v njegovem primeru dalo jasen zgled, da takšnih dejanj ne bo toleriralo.

Dokumenti PDF postajajo vse pogostejši način za širjenje nevarnih programov. V kolikor jih prejmete iz neznanih virov, jih ne odpirajte, prepričate pa se tudi, da uporabljate zadnje verzije programov Adobe za branje ali urejanje



omenjenih dokumentov. Isto velja upoštevati tudi za vso ostalo programsko opremo, ki je pogosta tarča izrabljanja varnostnih lukenj. Redno posodabljajte tudi svoj operacijski sistem in protivirusni program. Ob odmevnejših medijskih dogodkih pa bodite še posebej previdni pri odpiranju povezav in priponk v elektronski pošti, ki takšne dogodke oglašuje.

Ena od bistvenih prednosti ESETovih varnostnih rešitev pred konkurenco je v tem, da poleg virusnih definicij uporabljajo tudi napredno proaktivno zaščito, ThreatSense. Ta poskrbi, da ste varni tudi pred grožnjami takoj ob izbruhu, saj škodljivo kodo analizira in prepozna v realnem času tudi, če grožnja med virusne definicije še ni dodana. (P.R.)