



Win32/Conficker.X

Conficker.X je nova različica črva Confiker, ki se po internetu širi z neverjetno hitrostjo. ESET-ovi razvijalci trdijo, da gre za eno od najresnejših groženj v zadnjem času. Poleg izkoriščanja varnostnih lukenj v operacijskem sistemu Windows za širjenje po internetu, se črv širi tudi s pomočjo izmenljivih medijev, kot so USB ključki.

Črv je napisan tako, da okužen računalnik vključi v ogromno mrežo okuženih računalnikov (botnet). Avtorji črva imajo nad tem omrežjem popoln nadzor, iz okuženih računalnikov pa lahko izvajajo napade ali pošiljajo neželjeno pošto in zlonamerne programe. V tem omrežju se trenutno nahaja okoli dva milijona okuženih računalnikov.

Nova različica črva je posebna tudi v tem, da bo s 1.4.2009, navodila in posodobitve sposobna prejemati iz ogromnega števila domen, ta številka bi lahko po nekaterih predvidevanjih dosegla kar 50.000 domen na dan (prejšnje različice črva so bile sposobne komunikacije z 250 domenami na dan)! Strokovnjaki zaenkrat ne vedo, kakšne so namere napadalcev, predvidevajo pa, da bi lahko avtorji napadli kar infrastrukturo interneta.

Črv Conficker nedvomno predstavlja eno od najnevarnejših groženj v zgodovini interneta, saj je v kratkem času sposoben okužiti ogromno število računalnikov. Cilj napalcev je zgraditi čim večjo mrežo okuženih računalnikov, nato pa izvesti masoven napad na samo strukturo interneta ali izvajati obsežne vohunske dejavnosti.

Obnašanje črva Win32/Conficker.X na okuženem računalniku:

- Spremeni DNS nastavitve in onemogoči vsa varnostna orodja
- Onemogoči protivirusno programsko opremo
- Sposoben je komunikacije preko omrežja peer-to-peer (P2P)
- Od 1.4.2009 bo navodila in posodobitve sprejemal iz 50.000 domen na dan

Kako se zaščititi?

Svoj operacijski sistem Windows posodobite z vsemi varnostnimi popravki in poskrbite, da bo vaš protivirusni program posodobljen z zadnjimi virusnimi definicijami. ESET je bil pri odkrivanju novih različic črva Conficker s svojo proaktivno zaščito 100% uspešen.