Küberkurikaelte uus tööriist TDL-4 viskab konkureerivad pahalased välja

14 aastat tagasi - 09.07.2011 Autor: AM

Küberkriminaalide hetkel kõige täiuslikum tööriist TDSS (Kaspersky Labi rakendused tuvastavad seda sellise nimega, või ka TDL) loob miljonitest zombiarvutitest koosneva robotvõrgu ning sokutab kasutajate arvutitesse töövahendeid, millega saavad küberkriminaalid nakatunud arvutist spämmida, omanikult raha välja nõuda või programmi omanike jaoks ebasoovitavaid programme eemaldada. Uues versioonis on ka võimalus välja rentida nakatunud arvuteid võrgus käimiseks 100 dollari eest kuus, et küberuritegude jälgi segada ja nakatanud arvuti omanik süüdlaseks teha.

Kahjurprogrammi uues versioonis TDL-4 toimunud muutused on suunatud sellele, et luua konkurentide ja viirustõrjetootjate eest maksimaalselt kaitstud robotvõrku, mis võimaldab teoreetiliselt juurdepääsu nakatunud arvutitele isegi siis, kui suletud on kõik käsuserverid, mida kurjategijad kasutavad zombiarvutite juhtimiseks.

Muuseas tekkis TDL-4s võimalus eemaldada nakatunud arvutist umbes 20 populaarset konkureerivat viirust, kirjutab Kaspersky Lab. Nende hulgas on sellised laialt levinud kahjurprogrammid nagu Gbot, ZeuS, Optima ja teised.

Seejuures paigaldab TDSS ise arvutisse umbes 30 lisautiliiti, mille hulka kuuluvad võltsviirustõrjeprogrammid, reklaami näitamis- ja rämpsposti saatmissüsteemid. Üheks oluliseks uuenduseks on võimalus nakatada 64-bitiseid operatsioonisüsteeme. Robotvõrgu juhtimiseks kasutatakse peale käsuserverite veel avalikku failivahetusvõrku Kad.

TDL-4 uueks funktsiooniks on ka võimalus avada puhverserver. Kurjategijad pakuvad teenusena võimalust nakatunud arvutite kaudu anonüümselt võrku pääseda ja küsivad selle eest umbes 100 dollarit kuus. Lihtkasutajale tähendab see aga, et tema arvuti kaudu võib keegi eemalolev isik teha õigusvastaseid tegusid ja kahtlus langeb temale - pahaaimamatule arvutikasutajale.

Nagu eelmised versioonidki, levib TDL-4 enamasti nn partnerprogrammide kaudu. Kahjurtarkvara autorid ei tegele nakatunud arvutite võrgu laiendamisega ise, vaid maksavad selle teenuse eest kolmandatele isikutele. Vastavalt tingimustele

makstakse partneritele 20-200 dollarit 1000 kahjurtarkvara paigalduse eest.

Vaatamata juhtserverite kaitsemeetmetele õnnestus Kaspersky Labi ekspertidel teha nakatunud arvutite üldstatistika. Tulemus näitas, et 2011. aasta esimese kolme kuuga nakatati TDSS-iga kogu maailmas üle 4,5 miljoni arvuti, neist enamik (28%) USAs.

Arvestades kahjurtarkvara ülaltoodud paigaldushindu, võib hinnata küberkurjategijate umbkaudseid kulusid, et luua USAs arvutititest robotvõrk: see on umbes 250 000 dollarit.

“Me ei kahtle, et TDSS-i arendamist jätkatakse”, kinnitavad uurimuse autorid, Kaspersky Labi eksperdid Sergei Golovanov ja Igor Sumenkov. “Kahjurprogramm ja nakatunud arvuteid ühendav robotvõrk toovad arvutikasutajatele ja IT-spetsidele veel kuhjaga ebameeldivusi. TDL-4 koodi aktiivne arendamine, rootkit 64-bitistele süsteemidele, käivitumine veel enne operatsioonisüsteemi starti, Stuxneti arsenalist pärit teadaolevad rakenduste turvaprobleemid, P2P-tehnoloogiate kasutamine, isiklik viirustõrjeprogramm ja palju, palju muud paigutavad kahjurprogrammi TDSS tehnoloogiliselt kõige enam arenenud ja väga keerukat analüüsi nõudvate programmide hulka”.

Illustratsioon: Salvatore Vuono / FreeDigitalPhotos.net

- Uudised
- Turvalisus