Novi Storm prepoznaje virtualne strojeve

Novije inačice Storm crva sadrže tehniku detekcije da li se izvode na virtualnom stroju i u skladu s time mijenjaju svoje ponašanje. Sigurnosni stručnjak Bojan Ždrnja koji radi za SANS-ov Internet Storm Center (ISC) tvrdi da je ova inovacija dokaz raširenosti korištenja virtualizacije i sofisticiranosti programera malicioznog softvera.

Glavni cilj zlonamjernih korisnika je otežavanje analize novih inačica ovog crva, jer sigurnosni stručnjaci uobičajeno koriste virtualne strojeve kako bi sigurno izvršili i analizirali maliciozni kod. Ako Storm prepozna da se izvodi na VMware ili Virtual PC stroju, prekida svoje maliciozne aktivnosti i ponovno pokreće operacijski sustav.

Kako bi analizirali nove inačice Storm virusa, sigurnosni stručnjaci moraju ih pokrenuti na računalu bez korištenja virtualnih strojeva, promijeniti postavke virtualnih strojeva kako bi se onemogućila njihova detekcija ili koristiti tehnike ručne analize malicioznog koda. Storm je trenutno najaktivniji maliciozni softver koji se širi na Internetu slanjem e-mail poruka s lažiranim elektroničkim razglednicama koje zapravo korisnika vode na maliciozna web sjedišta.

pet, 2007-07-27 10:38 - Uredništvo**Vijesti:** CERT [1]
Kategorije: Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/262

Links
[1] https://sysportal.carnet.hr/taxonomy/term/9
[2] https://sysportal.carnet.hr/taxonomy/term/30