

Uusi näkymätön uhka tietokoneita vastaan

11.1. 10:39 (päivitetty 10:53) — Kalevi Nikulainen

Panda Securityn viruslaboratorio PandaLabs on tunnistanut useita rootkiteja (MBRtool.A, MBRtool.B, MBRtool.C) sisältäviä troijalaisia.

Rootkitit on suunniteltu vaihtamaan pääkäynnistyslohko (master boot record), eli kovalevyn ensimmäinen tai nollasektori, omaansa. Tämä on uusi tapa hyödyntää rootkiteja. Niihin liittyviä haittakoodeja on entistä vaikeampi tunnistaa.

- Tämä hyökkäystapa aiheuttaa sen, että rootkitien ja niiden piilottamien haitallisten koodien tunnistaminen on lähes mahdotonta sen jälkeen kun ne ovat asentuneet tietokoneelle, sanoo Luis Corrons, PandaLabsin johtaja.

- Ainoa tapa puolustautua on tunnistaa rootkitit ennen kuin ne pääsevät koneelle. Jos vastaavia haitallisia koodeja ilmaantuu jatkossakin, on olennaista käyttää proaktiivisia suojaustekniikoita, jotka voivat tunnistaa myös tuntemattomat uhkat.

Rikolliset hyödyntävät rootkiteja piilottaakseen haittaohjelmien toiminnot, jolloin ne ovat hankalia tunnistaa. Tähän asti rootkitit on asennettu järjestelmäprosesseihin, mutta PandaLabsin nyt tunnistamat rootkitit asennetaan sellaiselle kovalevyn osiolle joka käynnistyy jo ennen käyttöjärjestelmää.

Kun tällainen rootkit käynnistyy, se tekee kopion olemassa olevasta pääkäynnistyslohkosta, ja muokkaa sitä haitallisiin tarkoituksiin sopivaksi. Jos pääkäynnistyslohkoon yritetään päästä käsiksi, rootkit ohjaa edelleen alkuperäiseen versioon, jolloin käyttäjä tai sovellukset eivät huomaa mitään epäilyttävää.

Kun tietokone käynnistetään, muokattu pääkäynnistyslohko käynnistyy ennen kuin käyttöjärjestelmä on latautunut. Sillä hetkellä rootkit suorittaa loput koodistaan, jolloin se voi piilottaa itsensä ja siihen liittyvän haittakoodin täydellisesti. Tähän saakka rootkiteja on käytetty piilottamaan sovelluslaajennuksia tai prosesseja, mutta nyt löydetyt versiot voivat huijata järjestelmää suoraan. Sijainnin ansiosta käyttäjät eivät huomaa mitään poikkeavaa järjestelmän prosesseissa, sillä muistiin ladattu rootkit monitoroi pääsyä

levylle taatakseen haittaohjelmien huomaamattomuuden.

Pandan mukaan käyttäjien on hyvä suojautua tätä uudentyyppistä uhkaa vastaan. Erityisesti kannattaa jättää tuntemattomilta tahoilta tulevat tiedostot avaamatta.

Tämän haittakoodin poistamiseksi käyttäjien tulee käynnistää kone käynnistys cd:n kanssa. Tällöin pääkäynnistyslohkoa ei käynnistetä. Sen jälkeen pääkäynnistyslohko palautetaan esimerkiksi fixmbr:n avulla Windowsin Recovery Consolen kautta.

- Nämä rootkitit toimivat myös muilla alustoilla, kuten Linuxilla, sillä niiden toiminta on riippumatonta siitä, mikä käyttöjärjestelmä koneelle on asennettuna, lisää Corrons.

<http://www.digitoday.fi/tietoturva/2008/01/11/uusi-nakymaton-uhka-tietokoneita-vastaan/2008955/66>