

Kiristyshaittaohjelmaa levitetty aktiivisesti - Windows-järjestelmien välitön päivittäminen tärkeää

Metropoliassa tietokoneiden päivittymisen varmistaminen aloitettiin lauantaina iltapäivällä. Tietohallinnon hallinnassa olevista tietokoneista valtaosa on päivitetty viikonlopun aikana. Loput hallinnassa olevat tietokoneet tulevat päivittymään, kun koneet käynnistetään ja ne kytkeytyvät verkkoon.

Haittaohjelma on levinnyt ainakin sähköpostin liitetiedostoina. Sähköposteista on ollut useita versioita, joissa on ollut tekaistuja laskuja, työtarjouksia, tietoturvaravitteitä tai muita virallisen näköisiä tiedostoja. Kuten normaalistikin, käyttäjiä ohjeistetaan välttämään epämääräisten liitteiden avaamista sähköpostista.

Haittaohjelman leviäminen on jo pysähtynyt, mutta se on helppo muokata niin, että se lähtee uudelleen käyntiin.

Ratkaisu- ja rajoitusmahdollisuudet:

Kaikki Microsoft Windows -käyttöjärjestelmillä varustetut työasemat ja palvelimet on syytä päivittää mahdollisimman pikaisesti kaikilla saatavilla olevilla suojauspäivityksillä, mukaan lukien tiistaina 9.5.2017 julkaistut päivitykset.

Käytettävissä olevien tietojen perusteella kiristyshaittaohjelma ei aktivoidu ja pysty leviämään organisaation sisäverkossa, jos kaikki päivitykset on asianmukaisesti asennettu.

Microsoft on julkaissut korjauksia maaliskuun suojauspäivitysten yhteydessä korjattuun SMB-haavoittuvuuteen myös käyttöjärjestelmille, joiden tuki on jo loppunut, mukaan lukien Windows XP. Kyseinen päivitys on syytä asentaa viipymättä.

Toimiva ja testattu varmuuskopiointi on tehokas tapa varmistaa tehokas palautuminen kiristyshaittaohjelmatartuntatapauksissa.

Viestintäviraston tiedote asiasta:

<https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2017/varoitus-2017-02.html>