

## Haittaohjelma naamioitiin Microsoftin paikkaukseksi

27.7.2010 13:55 — Tuomas Linnake  
[tuomas.linnake@digitoday.fi](mailto:tuomas.linnake@digitoday.fi)

Windowsin pikakuvakeaukkoon hyökkäävät haittaohjelmat lisääntyvät. F-Secure mainitsee uusimpina tulokkaina muualta tutut vitsaukset nimeltä Sality ja Zeus.

Hyökkäykset Windows-käyttöjärjestelmän edelleen korjaamattomaan pikakuvake- eli Ink-haavoittuvuuteen lisääntyvät. Tietoturva-[F-Secure kertoo uusista haittaohjelmista](#) blogissaan. Entisten uhkien joukkoon liittyivät Sality ja Zeus.

Sality-perhe on ollut hyvin yleinen haittaohjelmien tartuttaja jo pidemmän aikaa. Myös Zeus lukuisine muunnelmineen on kiusannut pitkään.

F-Secure kertoo uusimman Zeusin leviävän roskaposteissa, jotka tekeytyvät Microsoftin paikkaustiedotteeksi. Viestissä varoitetaan uudesta madosta, ja liitteenä on tietoturvapaikkauksen sijaan haittaohjelma.

Zeus on usein hankala torjuttava, mutta F-Secure ei usko tämän Zeusin muunnelman leviävän tehokkaasti. Zeus varastaa uhrin tietoja vakoilemalla näppäimistön painalluksia. Samaa tekee tuore haittaohjelma Chymine, jonka havaittiin iskevän Windows-aukkoon viime viikolla.

### Tilanne vielähallinnassa?

Heinäkuun puolivälissä havaittuun Windowsin [haavoittuvuuteen](#) tunkee myös vanhan Vobfus-perheen uusi versio. Ensimmäisenä pikakuvakkeiden käsittelyongelmaan tarttui kuitenkin Stuxnet-niminen rootkit-ohjelma, joka osaa hyökätä Siemensin tehdasjärjestelmiin.

F-Secure kiteyttää tilanteen hyvät ja huonot puolet.

- Huono uutinen on se, että useat uudet haittaohjelmaperheet yrittävät nyt hyödyntää Microsoftin Ink-haavoittuvuutta. Hyvä uutinen on, että toistaiseksi me ja useat muut virustorjujat tunnistamme uudet hyväksikäyttönäytteet.

---

Helppo tunnistettavuus johtuu F-Securen mukaan siitä, että uudet haittaohjelmakuormat käyttävät hyväkseen samaa perusluonteista hyväksikäyttömenetelmää kuin aiemmatkin Ink-uhat. Hyväksikäyttömenetelmästä ei ole havaittu uusia versioita.

<http://www.digitoday.fi/tietoturva/2010/07/27/haittaohjelma-naamioitiin-microsoftin-paikkaukseksi/201010345/66>