

## KRP tutkii salasananvuotoa, krakkerit ovat Magical Pink Bear & ZeroPoint

14.10.2007 20:24 — Kalevi Nikulainen

Lähes 80 000 suomalaisen käyttäjätunnuksia ja salasanoja koskevan vuodon poliisitutkinta on keskitetty Keskusrikospoliisin tietotekniikkarikosyksikköön, kertoo Viestintäviraston tietoturvayksikkö CERT-FI.

**CERT-FI:n mukaan** asianosaisten palvelutarjoajien olisi syytä harkita rikosilmoituksen tekemistä paljastuneiden tietojen vuoksi suoraan KRP:lle.

Ensimmäinen CERT-FI:n tietoon tullut salasanan tiedostoa jakanut www-sivusto on sulkeutunut sunnuntaina aamuyöstä Suomen aikaa. Tiedosto on nyt sijoitettu sunnuntaipäivän aikana useille uusille www-sivustoille ja vertaisverkkopalveluihin. Tämä osoittaa internetin luonteen: kerran julkaistua tietoa on käytännössä mahdotonta saada pois verkkojaketusta täydellisesti.

CERT-FI on vastaanottanut runsaasti kyselyitä tiedoston sisällöstä, murretuista palvelimista ja toimintamenettelyistä tilanteessa.

CERT-FI:n käsityksen mukaan tiedostossa ei ole pankkipalveluihin liittyviä käyttäjätunnuksia ja salasanoja.

Yksikön Irc-gallerian ylläpidolta saaman tiedon mukaan sen palvelimille ei ole murtauduttu. Joukko tiedostossa listattuja muista verkkopalveluista kaapattuja käyttäjätunnus-salasanapareja on toiminut myös Irc-galleriassa. Näiden listaan täsmäävien Irc-galleria -tunnusten salasanat on nollattu, ja käyttäjiä ohjeistetaan sisäänkirjautumisen yhteydessä hankkimaan uusi salasana.

**Bat.org** on julkisesti ilmoittanut joutuneensa tietomurron kohteeksi ja palvelu on ajettu huollon ajaksi  
alas **Kiekkoliiga.net** on julkisesti ilmoittanut joutuneensa tietomurron kohteeksi **Rakkausrunot.fi** on julkisesti ilmoittanut joutuneensa tietomurron kohteeksi **Battlefield.fi** on julkisesti ilmoittanut joutuneensa tietomurron kohteeksi

---

**mesenet-galleria.com** on julkisesti ilmoittanut joutuneensa tietomurron kohteeksi **hilavitkutin.com** on julkisesti ilmoittanut asiakkaidensa käyttäjätunnustietoja löytyneen julkistetulta listalta **voitta.net** on julkisesti ilmoittanut joutuneensa tietomurron kohteeksi

Jotkut listalla mainitut käyttäjätunnukset ovat toimineet myös käyttäjän sähköpostipalvelun tunnuksina. Samaa salasanaa ei ole suositeltavaa käyttää eri palveluissa.

Launataina verkkoon ladattiin 4.5 megatavun tekstitiedosto (passlist.txt). Se sisältää käyttäjänimiä, sähköpostiosoitteita, salasanoja ja md5/sha1-salasanatiivisteitä, ja koskee noin 79 000 suomalaista akäyttäjää. Levittäjiksi ilmoittautui kaksi ihmistä Ruotsista, mutta verkossa epäiltiin, että krakkerit ovat suomalaisia.

**Kyseessä on lähinnä** keskustelufoorumien tai yhteisöpalvelujen käyttäjätunnuksia sekä käyttäjätunnusten md5 / sha1 -salasanatiivisteitä. Tiedostossa näyttäisi olevan myös joitakin satoja selväkielisiä salasanoja.

CERT-FI selvittää parasta aikaa, mihin palveluihin tunnuksset mahdollisesti liittyvät. CERT-FI on myös yhteydessä verkkopalveluntarjoajiin, teleyrityksiin ja poliisiviranomaisiin.

Omat tunnuksset voi tarkistaa tiivisteistä vapaasta [tiedostosta](#).

**Verkossa oli** seuraavanlainen kirjoitus salasanapaljatuksen seurauksista:

"Esimerkiksi meikäläisen kohdalla tietyt "nettitunnuksset" avaisivat ongelmalapselle oven kaikkiin koulutöihini, opintosuunnitelmaani, kurssi-ilmoittautumisiini jne. sekä koulun tietokoneverkkoon. Olisi siinä kiva, kun ensin kaikki tentti-ilmoittautumiseni oltaisiin peruttu ja sen jälkeen nimissäni tehty koulun verkossa niin paljon pahaa, että poliisit tulisivat ovelle koputtelemaan. Eikä tuo vielä mitään - sähköpostin kautta saisi avaimet käytännössä kaikkiin käyttämiini maksullisiin ja maksuttomiin verkkopalveluihin nettipankkia lukuunottamatta (avainlukukortti lompakossa)."

**Ja tässä krakkeiden sanomiset**

"We cracked 78 000 (ok, almost 79 000) accounts around the net and of course we'd like to share them with you, right. Mostly finnish accounts, so maybe it would be better to have this prologue in finnish too.

---

Hei, lista pitää sisällään noin 29 800 MD5 hashia, muutamisen sataa SHA1 hashia, 33 000 kappaletta SMF foorumin hasheja ja toki myös muutamisen sataa salasanaa plaintextinä.

Joistakin puuttuu mailit, valitamme. Niitä joko ei ole ollut saatavilla tai ne ovat tarkoituksella jätetty pois. Kysymyksiä varmasti syntyy; "Miten teitte sen?", "Miksi olen listalla?", "Keitä te olette?".

Jos olet listalla, sori hei. Meillä ei ole varmastikaan ollut syytä satuttaa sua... tai sitten oli. Todennäköisesti olet vaan osunut väärään paikkaan väärään aikaan, mutta jokatapauksessa et olisi asialle mitään mahtanut.

79 000 hashiahan on siis käsittämätön määrä, ja vielä kun ne rajataan yhteen pieneen maahan niin todennäköisyys siihen että netti- tai koulukiusaajasi löytyy listalta on hyvin suuri. Mukaanhan tottahan toki mahtuu myös vaikka minkä yrityksenkin työntekijöitä ja webmastereita, joten vahinko mitä tällä listalla voi saada aikaan on myöskin suuri.

Me, the Magical Pink Bear & ZeroPoint olemme kahden hengen ruotsalainen hakkeriryhmä. Meihin ei toistaiseksi voi ottaa yhteyttä sähköpostitse tai IRCitse, syy lienee itsestään selvä."

**Jouko Pynnönen** käsittelee asiaa Digitoday [Ylivuoto](#)-blogissa.

<http://www.digitoday.fi/tietoturva/2007/10/14/krp-tutkii-salasanavuotoa-krakkerit-ovat-magical-pink-bear--zeropoint/200725450/66>