



Politsei- ja Piirivalveamet
keskkriminaalpolitsei

Märka ja reageeri

Reemo Salupõld



- Kas või millal peab teavitama
- Igast infost ei tule kriminaalmenetlust, kuid info on ikkagi vajalik
- Milliseid andmeid edastada
- Kriminaalmenetluse alustamine



Koosseisud



- **§ 206. Arvutiandmetesse sekkumine**

Arvutisüsteemis olevate andmete ebaseaduslik muutmine, kustutamine, rikkumine või sulustamine

- **§ 207. Arvutisüsteemi toimimise takistamine**

Arvutisüsteemi toimimise ebaseaduslik häirimine või takistamine andmete sisestamise, edastamise, kustutamise, rikkumise, muutmise või sulustamise teel

- **§ 216¹. Arvutikuriteo ettevalmistamine**

- **§ 217. Arvutisüsteemile ebaseaduslikult juurdepääsu hankimine**

Arvutisüsteemile ebaseaduslikult juurdepääsu hankimine kaitsevahendi kõrvaldamise või vältimise teel



Kes ees, see mees



Vaata seda:

[http://www.kyberkuritegu.com/watch?v=ewhjrf325tgy47seeonl
aheviirus.mp4](http://www.kyberkuritegu.com/watch?v=ewhjrf325tgy47seeonl
aheviirus.mp4)

Kui see ei tööta, siis proovi seda

[http://tahansinuarvutisse.com/käivitapalunmindggferhhthtjttjt.e
xe](http://tahansinuarvutisse.com/käivitapalunmindggferhhthtjttjt.e
xe)



Blackshades



Kriminaalasjas alustati menetlust 30.04.2014 KarS § 216`lg1 järgi selles, et 26.11.2011 otsid Blackshades Net kasutajad „fantomin75“ ja „Nebulos“ Blackshades Recovery tarkvara, mis oli loodud arvutikasutajate nimede ja paroolide kogumiseks nakatatud arvutitest ja automaatselt saatis kogutud andmed Blackshades serverisse.



Blackshades



„Fantomin75“

6166 erinevat kasutajanime ja parooli

400 erinevast seadmest

„Nebulos“

1587 erinevat kasutajanime ja parooli

107 erinevast seadmest.



Tootsi.ee



Ajavahemikul 22.12.2014 22:43 – 23.12.2014 9:40
toimus rünnak Siseministeeriumile kuuluvatel serveritel
asuva Tootsi valla kodulehe vastu (tootsi.ee), mille
käigus Eesti haldusallas asuv IP-aadress 123.243.265.12
tegi 350 000 päringut (ehk 9 päringut sekundis)
lokaalsel aadressil "/etc/passwd" asuva faili saamiseks.



Gmail



Loodetavasti jõuab see kiri teieni õigeaegselt. Käisin reisil Newcastle, Suurbritannia, ning reisi käigus varastati mu dokumendid, sealhulgas pass ja krediitkaart, mis olid minu kotis. Saatkond oli nõus abistama minu lennu organiseerimisega ilma passita, minu kanda jäi piletikulu ja hotelli arve. Paraku ei ole mul võimalik aga kontole ligi pääseda ilma pangakaardita ning pank ei ole suuteline nii kiiresti uut kaarti väljastama, et ma lennule jõuaksin ja hotelliarve tasutud saaksin. Antud olukorras olen sunnitud paluma lühiajalist laenu, mille saan tagasi maksta niipea kui koju tagasi jõuan. Vajan summat mis oleks 1000 Euro, et katta oma kulud. Kui oleks võimalik raha saata Western Union kaudu, siis see oleks kõige parem. Vabandan ebamugavuse pärast, aga mul on vaja jõuda järgmisele lennule ja igasugune abi on teretulnud. Kui on võimalik aidata, siis saadan oma konto andmed.

Vastust ootama jäädes.

Reemo



Gmail



Perioodil 2014 detsembri lõpp – 2015 veebruari algus said kõrvalised isikud juurdepääsu erinevate Eesti kodanikke Gmail kontodele (13) ning saatsid nende kontaktidele identse tekstiga (mille sisuks oli rahalise abipalve) e-kirju. Selle tulemusena on 2 isikut kandnud kurjategijate poolt saadetud WU (Western Union) rekvisiitidele üle raha.





cybercrime@politsei.ee

