

# Nederlandse server bron van malware

By Erik Van Der Walle, [www.nrc.nl](http://www.nrc.nl)  
augustus 31ste, 2017

Ruim 700 miljoen e-mailadressen die opgeslagen lagen op een Nederlandse server, zijn gebruikt om spam mee te verzenden. De gegevens werden op illegale wijze verzameld.

Dat meldde het weblog *Troyhunt* van de Australiër Troy Hunt woensdag. Hunt is een expert op het gebied van (on)veiligheid op het web. Het gaat om een van de grootste datalekken ooit. Op de openbare server lagen talloze lijsten opgeslagen met daarin zo'n 711 miljoen unieke e-mailadressen. Naast e-mailadressen waren in de lijsten ook bijbehorende wachtwoorden opgenomen. De server was door een beveiligingsfout zonder wachtwoord toegankelijk.

Bezoekers konden de data downloaden zonder eerst te hoeven inloggen.

De gegevens werden vervolgens door een spambot gebruikt om schadelijke software mee te versturen. Een spambot is software die ontworpen is om ongewenste berichten naar zo veel mogelijk mensen te versturen. De server met gegevens werd gevonden door een dataonderzoeker uit Parijs.

De inloggegevens werden ingezet bij een grootschalige malwareoperatie. Om spamfilters te omzeilen werd vanaf bestaande adressen mail verstuurd door bot 'Onliner'. Daarmee werd software vermomd als een bankupdate naar inboxen over de hele wereld verstuurd. Doordat de software afkomstig is van echte e-mailadressen herkennen veel spamfilters de frauduleuze software niet als zodanig. De bot Onliner heeft naar schatting tot zo'n tienduizend computerinfecties geleid.

Een deel van de gestolen gegevens is afkomstig uit eerdere lekken, zoals de LinkedIn-hack van 2012.

