soft solutions

VOIP - SOFTWARE - HARDWARE - INTERNET - CONSULTANCY

Soft Solutions
Ruijslaan 49
7003 BD Doetinchem
Nederland
Telefoon : 0314 36 04 47
Gsm : 06 55 806 940
Handelsreg. Arnhem nr. : 09051259
BTW : NL 0658 02 251B01
E-mail : info@softsolutions.nl
Website : www.softsolutions.nl

# Handleiding

## Voorkom infiltratie met ongewenste programma's: Outlook Express

Auteur: Henk Schuurman
**eerste uitgave: 8 november 2010**
**Wijzigingen:**

**Inleiding:**

Criminelen gebruiken verschillende methodes om uw PC te besmetten met “malware”, “spy-ware” en virussen. Waar het een “hacker” vroeger ging om de “sport” is het doel tegenwoordig altijd geld.

Een e-mail adres is geld waard, een “life” e-mailadres is het tienvoudige waard.
Bestanden met e-mail adressen worden duizenden keren verkocht en brengen veel geld op (zie pag. 8).
Het “hacken” van een PC is nog lucratiever. Gehackte PC’s worden in een botnet gekoppeld en worden zonder medeweten van de eigenaar gebruikt om duizenden e-mails per dag te versturen met als doel reclame te maken voor producten en/of PC’s te hacken om het botnet uit te breiden.

De eerste lijn van beveiliging is anti-virus programmatuur.
Goede programma’s zijn Nod32 of Kaspery

De tweede lijn is de gebruiker: U! Wanneer u niet goed oplet wat u doet kan geen virusprogramma u redden.

**Hoe raakt uw PC besmet:**

**Met een virus of malware:**
U ontvangt een e-mail waarin de afzender(*) gegevens heeft geplaatst waarin een virus of een download-programma is verborgen Deze gegevens kunnen eruitzien als een foto, een icoon, een link, of andere data die vanaf een web-site worden ge-download.
Door de e-mail te selecteren (aan te klikken) wordt het download-programma actief en laadt en installeert andere programma’s die de afzender de controle geven over uw PC.
Wanneer de signatuur van het download-programma bekend is en uw anti-virus programma is up to date kan het download-programma herkend en verwijderd worden; zo niet dan is uw PC besmet.

Op pagina 3 in de handleiding wordt getoond, hoe u kunt voorkomen dat een download-programma actief wordt.

(*) De afzender is niet de naam die vermeld staat. Door “spoofing” wordt de naam van de afzender vervangen door een ander e-mail adres;

**Met een link naar een besmette website:**
Omdat de anti-virus programmatuur steeds intelligenter en beter wordt, maken criminelen steeds vaker gebruik van nieuwsgierigheid en onkunde van gebruikers. Nog steeds openen mensen iedere e-mail die ze ontvangen, met als gevolg..... En ook het tonen in het “preview” venster kan gevolg hebben.

Er worden ook e-mails verstuurd die zo echt lijken op onder andere e-mails van banken, UPS, of een sociaal netwerk dat mensen het onderscheid niet meer zien. Door op een link in de e-mail te klikken worden ze doorgestuurd naar een besmette website en ..... het kwaad is geschied.

Ik laat hier zien hoe u een e-mail kunt onderzoeken zonder deze te selecteren en hoe u kunt herkennen of een e-mail afkomstig is van de vermelde afzender.

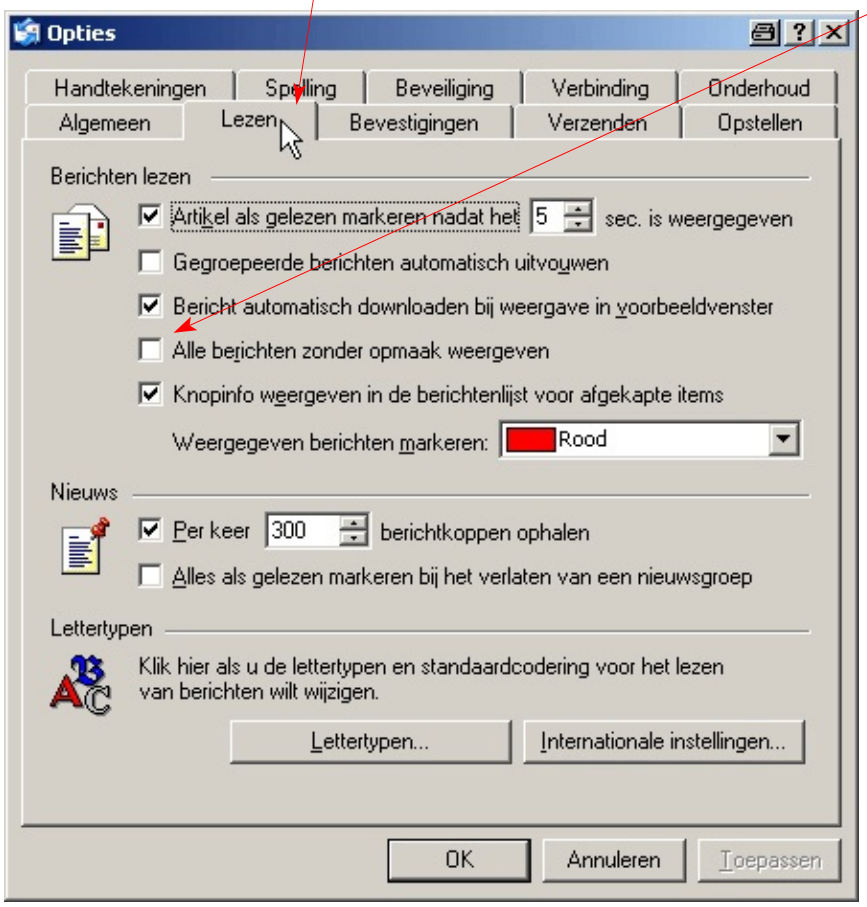
Maar we beginnen met een instelling in Outlook en Outlook Express die iedereen zou moeten in-activeren, zodat er niet zomaar programma’s op uw PC kunnen worden gezet.

**Configureer Outlook Express zodat er geen programma's worden gedownload:**

Klik op Extra Opties


Klik nu op het tabblad Lezen en de-selecteer de keuze Alle berichten zonder opmaak weergeven




Elk e-mail bericht wordt nu als tekst document weergegeven. Geen mooie franje, foto's of logo's die vanaf een website worden ge-download. Pas als blijkt dat een e-mail te vertrouwen is klikt u op de boodschap boven in de e-mail (zie volgende pagina)

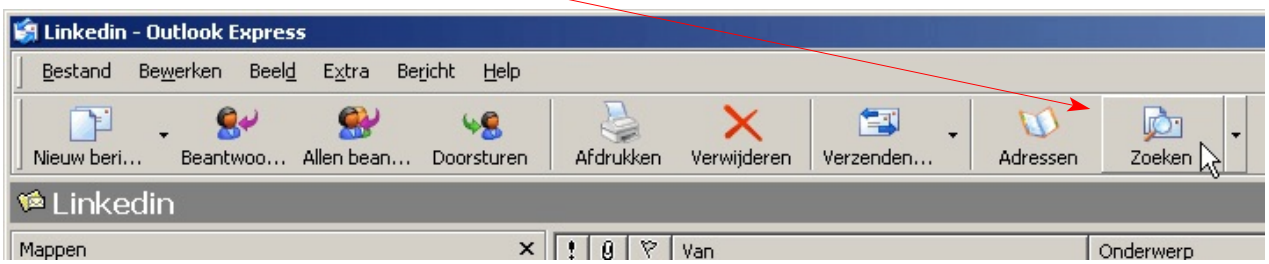
 

Wanneer u zeker weet dat een e-mail authentiek en te vertrouwen is klikt u op de boodschap

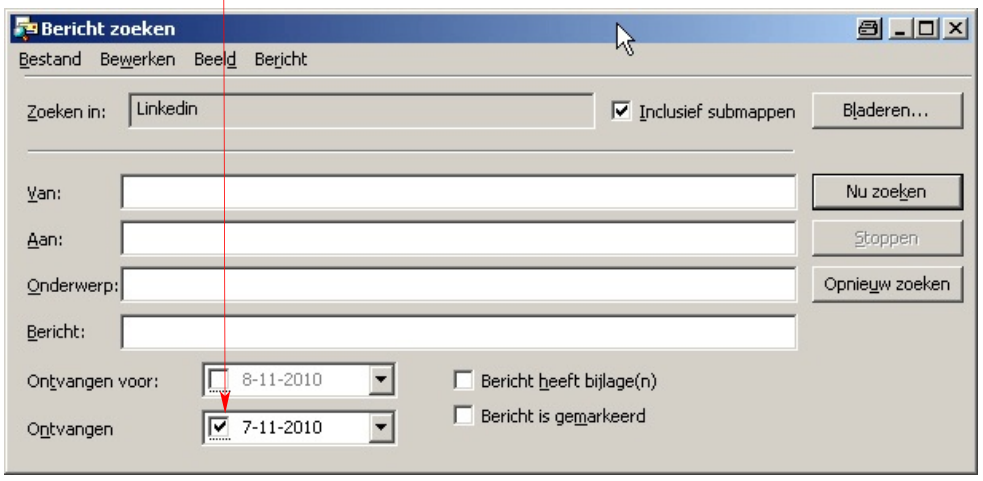

**Hoe herkent u een foute e-mail:**

Om te kunnen onderzoeken of een e-mail fout is, zal deze moeten worden geselecteerd. Dit kan niet in het normale venster, omdat dan programma's ge-download kunnen worden. Daarnaast herkent u niet of het een gefingeerde e-mail is.
Er is één plek waar u dit zonder gevaar kunt doen: In het zoekvenster.

**Selecteren van e-mail:**
Klik op het icoon Zoeken

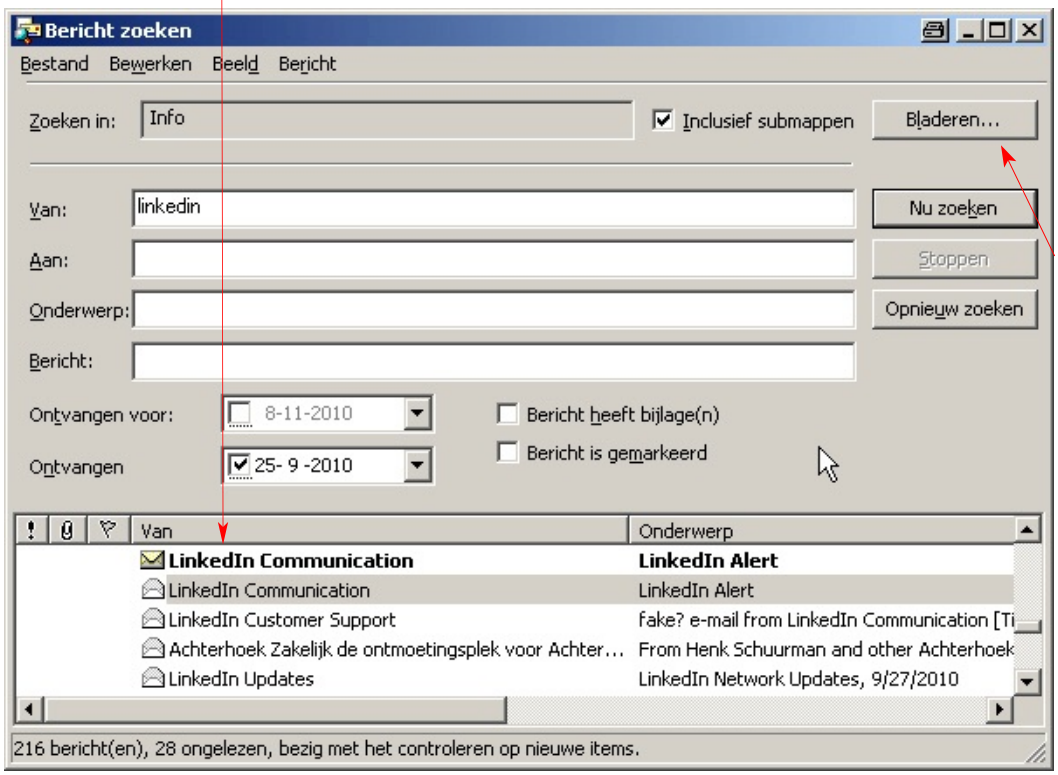



Klik nu op Ontvangen en selecteer een datum

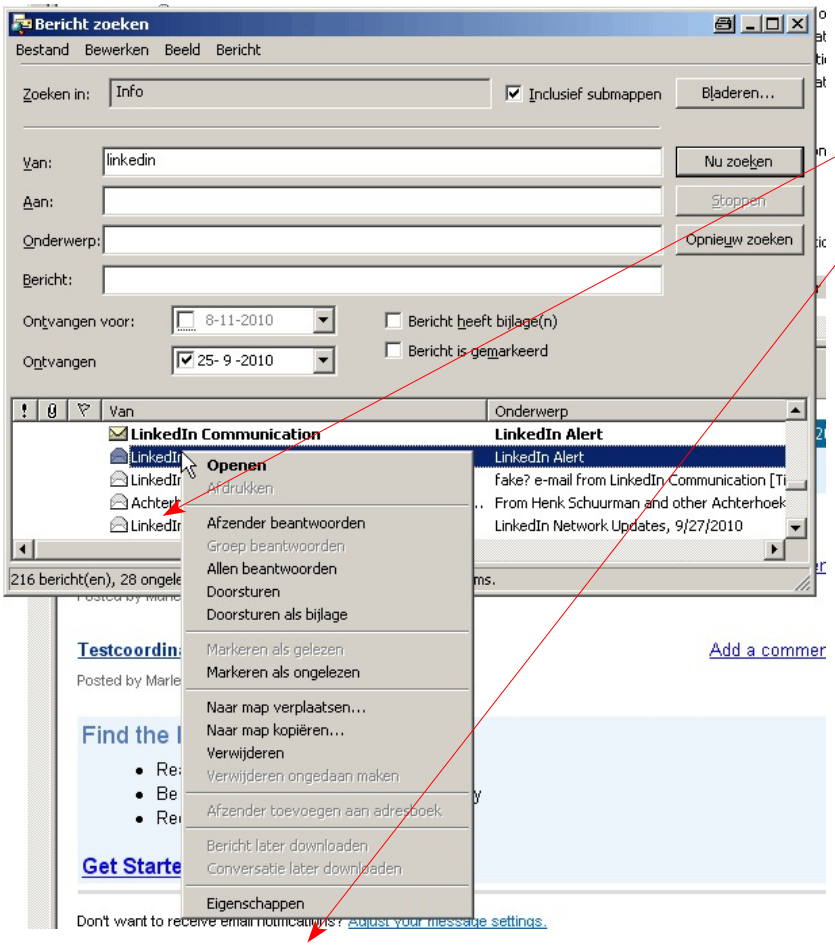


U ziet nu alle e-mail in de map vanaf de geselecteerde datum.

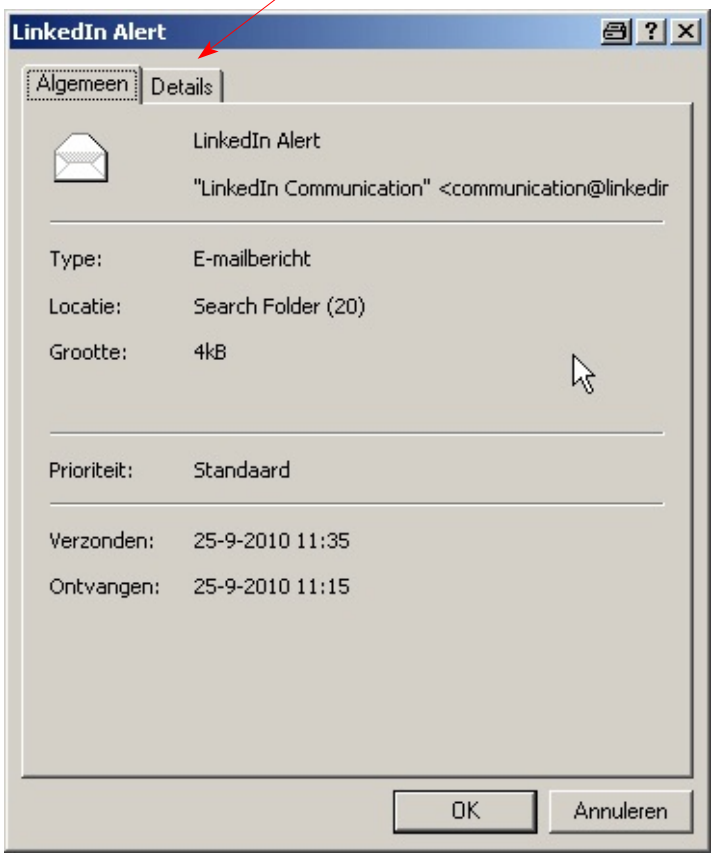


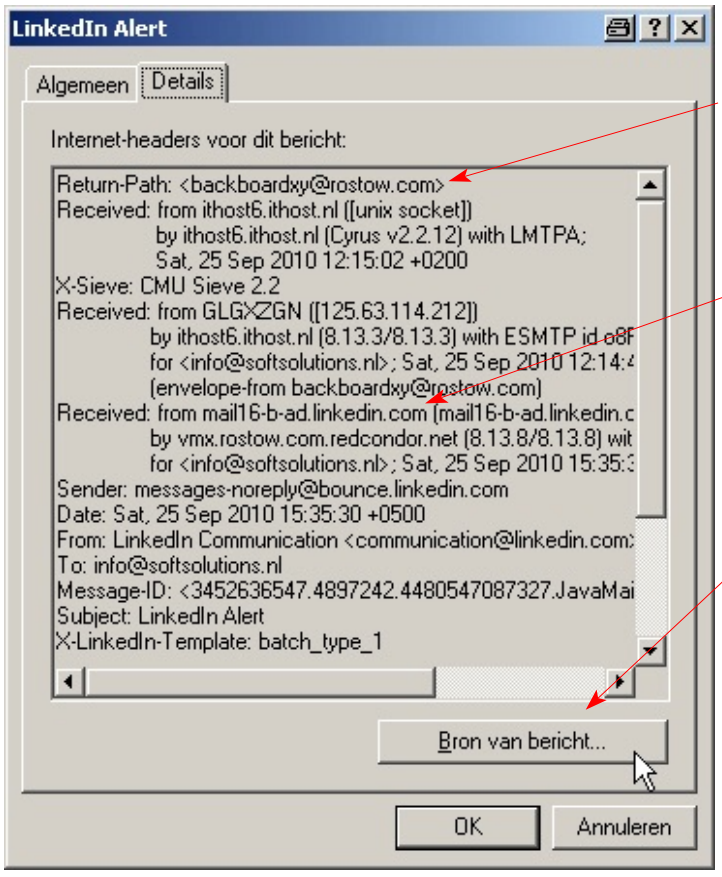

Om er zeker van te zijn dat u geen foute e-mail selecteert start u het zoeken in een map met vertrouwde e-mail. Klik op Bladeren om de map te selecteren waarin de te onderzoeken e-mail staat.




Klik met de rechtermuis toets op de te onderzoeken e-mail en kies Eigenschappen

Klik op het tabblad Details



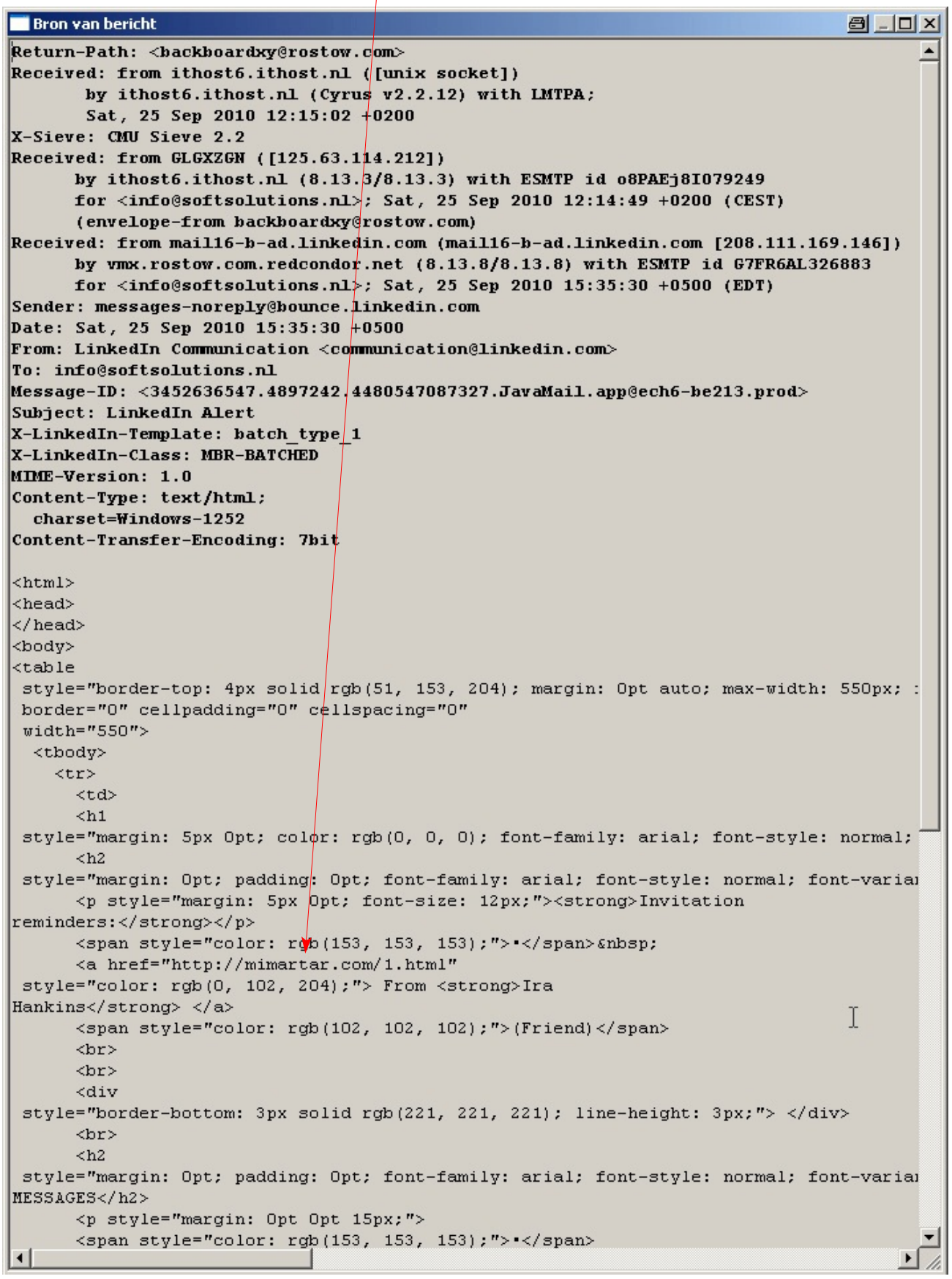

De bovenste regel van de e-mail laat het **Return-Path** zien. Dit komt niet overeen met de afzender en is dus een verwijzing naar een oneigenlijk of crimineel gebruikt adres.

Het tweede **Received** adres is ook vals: er staat mail16-b-ad.linked .com en dat is niet juist.

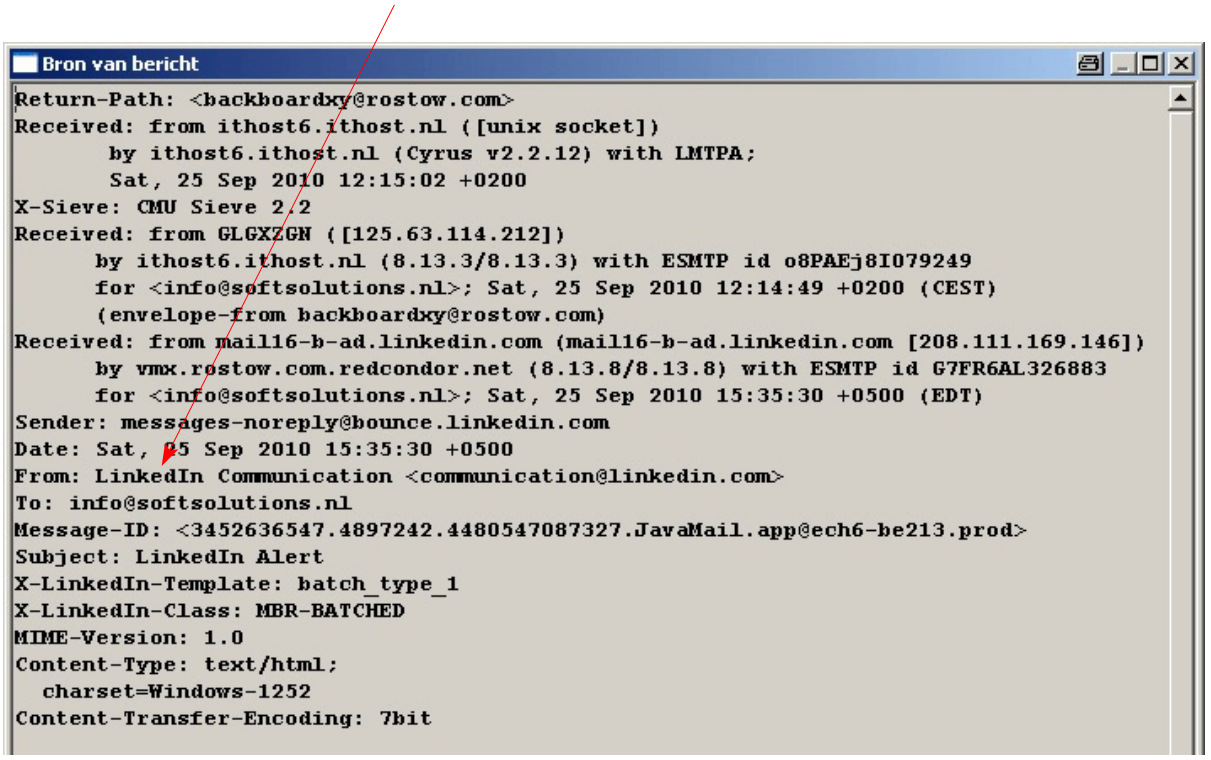
U hoeft nu al niet verder te kijken, deze e-mail is vals en probeert u ertoe te verleiden iets te doen wat u niet wilt.

Klikt u op Bron van bericht dan krijgt u de volledige inhoud van de e-mail te zien.

In de bron van het bericht ontdekt u nog meer zaken die niet kloppen:
De link in de e-mail verwijst naar mimartar.com. Deze website is met zekerheid besmet.



Laat u niet verleiden door de tekst **From: LinkedIn Communication ....**




Dit is niet meer dan tekst en door de samensteller van de e-mail gebruikt om u te misleiden.

**Resumé:**
Selecteer niet zomaar een e-mail; 90% van alle e-mail is van twijfelachtige of zelfs criminele afkomst en kan gevaar opleveren voor de ongestoorde werking van uw PC.

**Is het moeilijk om deze instructies uit te voeren?**
Nee; wanneer u dit een aantal keren op de getoonde wijze doet, hebt u al snel door waar u op moet letten. Het is een manier van werken die noodzakelijk is geworden omdat er voor criminelen heel erg veel geld valt te verdienen.
Het laatste botnet dat in Nederland is opgerold bestond uit 15 servers van een Nederlandse provider en meer dan 30.000.000 PC's. Iedere PC verstuurde meer dan 5.000 stuks e-mail per dag, met een opbrengst van 0,01 eurocent per e-mail.

***Verdienste meer dan € 15.000,00 per dag;***

Met als enige kosten de tijd die nodig is om een programma te schrijven die PC's hackt en in een botnet schakelt.

**Is het belangrijk om uw e-mail te beveiligen?**
Ja; dezelfde man achterhaalde zo ook toegangscodes en wachtwoorden naar bankrekeningen. Deze schade is niet uitgezocht omdat de banken geen uitsluitsel wilden geven, maar € 100.000.000 is voor de banken een schijntje, waar ze zich niet druk om maken!

**Wilt u meer zekerheid??..... Laat ons dan advies uitbrengen.!!**