

19 April 2007

Annex 2

On November 9, 2006 or earlier the Respondent changed registration details of my company's domain, direction.com through the registrar we then used: 000domains.com. The name of the registrant of direction.com was changed and so was the user id and the password giving access to the administrative interface at 000domains.com.

Shortly after the change, the following registration info was visible in 000domains customer database:

Registrant:

Rialex

Skovdalen 10

Nr. Snede, DK 8766

DK

Registrar: 000DOM

Domain Name: DIRECTION.COM

Created on: 21-DEC-95

Expires on: 19-NOV-07

Last Updated on: 09-NOV-06

Administrative, Technical Contact:

Exchange, Rial sillworks4@gmail.com

Rialex

Skovdalen 10

Nr. Snede, DK 8766

DK

45.7579999

Summary of the changes: Registrant name was changed. The email address belongs to the Respondent. The phone number was changed to a non-working number. The password at 000domains was changed.

When I from 000domains got an automatic notification that there had been changes to the registration of direction.com, I immediately responded by email and said I had not requested such changes. The reply back from 000domains read like this:

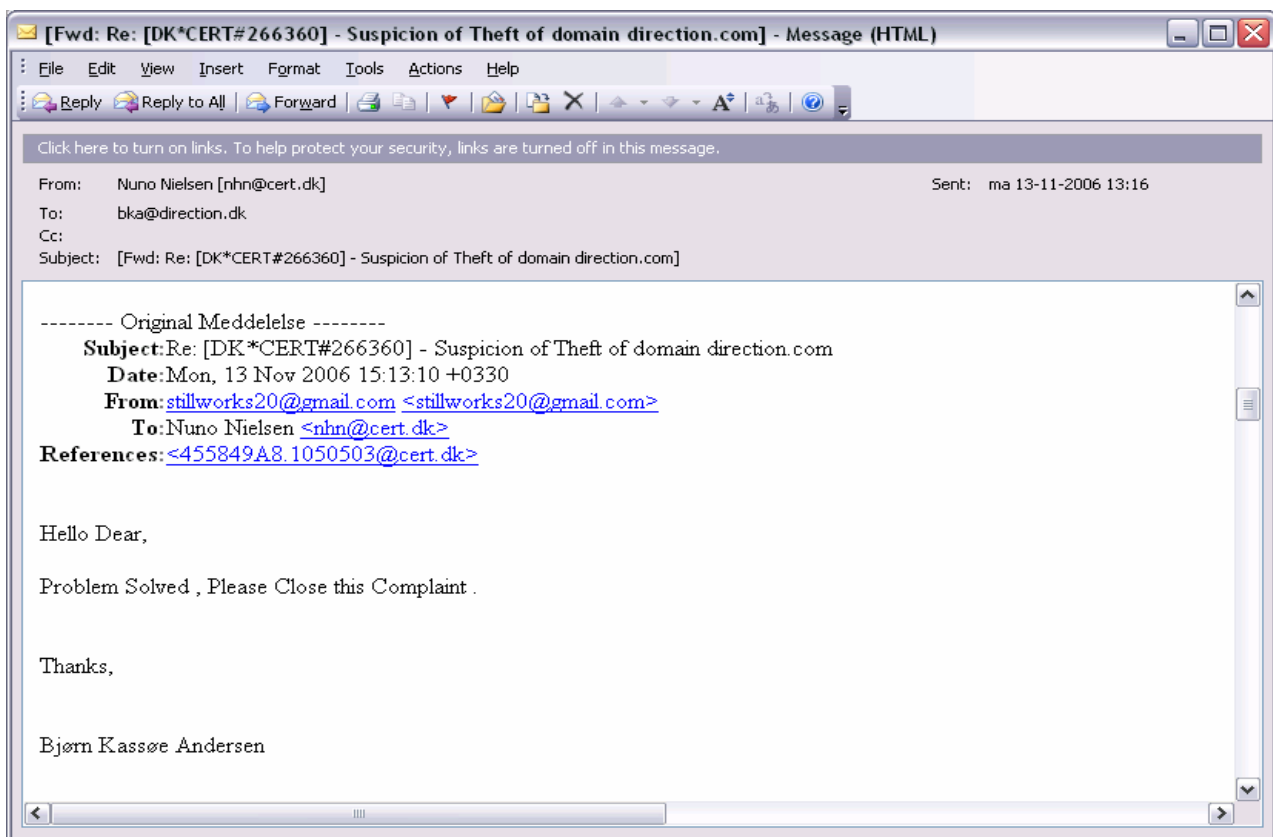
... it appears that the domain direction.com has been moved to a different account and the registrant information changed.

If you believe you have reason to dispute the ownership of a domain, you will need to go through the proper procedures to do so. Please see these links for more information on the Uniform Domain Name Dispute Resolution Policy. If you have any further questions about domain disputes, please contact legal@dotster.com.

Direction
Bjørn Kassøe Andersen
Skovdalen 10
DK-8766 Nr. Snede
Tlf. (+45) 75 77 03 30
Fax (+45) 75 77 03 39
bka@direction.dk
www.direction.dk

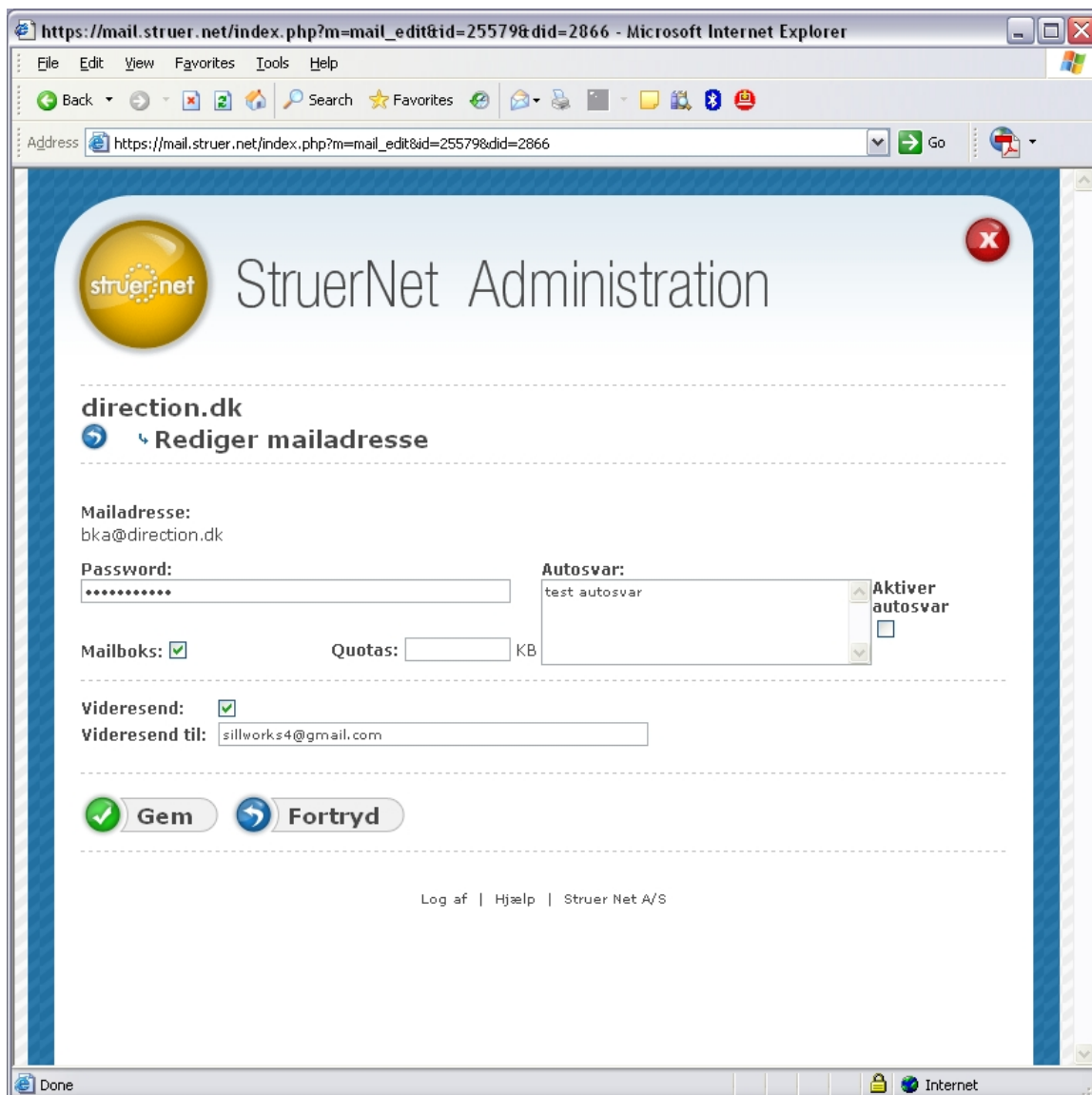
I was then in dialog with 000domains tech support. I provided documentation by fax so they could see I was the legal owner of direction.com and I again stated that I had not requested any changes.

I further contacted security experts at the Danish branch of CERT, www.cert.dk (affiliated with the CERT Coordination Center at Canegie Mellon University, www.cert.org). We ran full security checks of my company's computers and found no breaches or vulnerabilities. No spyware, keyloggers, root kits and so on. While we were investigating what had happened, it became clear that the Respondent was receiving copies of all my incoming mail. Surprisingly he or she revealed what was going on by trying to get CERT off the case in an email with the following wording in English: "Hello Dear, - Problem Solved. Please Close this Complaint. Thanks." and then my name written correctly with the use of Danish national characters. The wording can be seen in the following screendump:



The email was sent from the address stillworks20@gmail.com and CERT tracked the originating email server to a location in Germany. The mentioned email address is on the internet reported as being used by a domain name hijacker, see Annex 3.

Apparently the Respondent had gotten access to my direction.dk mail account which at that time was hosted by the Danish ISP struer.net. In the email account's webinterface it was visible that all my incoming email was being forwarded to sillworks4@gmail.com, cf. this screendump:



So far, my best guess is that struer.net has somehow been hacked. Struer.net finds that unlikely but they have not been able to produce any log files showing exactly what happened. I was not convinced that they had sufficient focus on it security and moved as fast as possible to another ISP.

Probably, the Respondent gained access to the domain registration account at 000domains by using the feature for resetting a password. The request for a new password would then be sent to my Danish email account with stealth forward to the Respondent's email address, sillworks4@gmail.com. If this was the way it happened, an unanswered question is how the 000domains-password could be reset without me seeing that it happened. Did the Respondent also have access to my webmail-interface at struer.net and did the Respondent delete incoming messages relating to a reset of password?

After a couple of days, the 000domains had rolled back the unwanted changes and I had apparently regained control of the direction.com domain name. The password for 000domain.com's web interface was of course changed and I also immediately changed my email contact address to new address at a

different provider, cutting my compromised Danish ISP, struer.net, out of all sensitive communication regarding this case.

In my dialog with 000domains I asked if they could raise their security level so that changes to my account would require more than "just" a hacker's access to my incoming email. This was not an option. Asking for higher security, 000domains tech support did offer to lock the domain. As I planned to move the domain to a different registrar, I did – unfortunately - not say yes to locking the domain. I thought that a new and stronger password with 000domains and use of a different ISP for email correspondence with an equally stronger password would be sufficient.

On January 18, 2007 I realized that I had again lost control of direction.com. This time changes to the ownership of the domain took place without any notification from 000domains or from the new registrar, 123cheapdomains.com which uses Tucows.com as registrar.

What had happened appears to be that the rollback made by 000domains.com tech support on November 13 had not taken into account that the Respondent already two days before, on November 11, initiated a transfer process to move direction.com to another registrar.

How it happened is clear from the following detailed description, provided to me by 000domain's legal department:

- 11/08/06: Someone at ip:217.219.63.254 logged into your account and changed the domain owner/admin/tech/bill contacts from Bjorn Andersen to Rial Exchange (with an email of sillworks4@gmail.com).
- 11/09/06: Someone at ip:217.219.63.254 logged into your account and moved this domain to a different account ("2nd account").
- 11/09/06: A few minutes later, someone at ip:217.219.63.254 logged into the 2nd account and moved the domain to yet another account ("3rd account").
- 11/11/06: The transfer authorization code was requested and sent to the admin contact email of record (sillworks4@gmail.com).
- 11/11/06: The domain transfer initiated/processed to Tucows based on transfer request confirmed by the admin contact email of record (sillworks4@gmail.com). Tucows' records and ours indicate that the admin contact email of record (sillworks4@gmail.com) was the requesting/approving email for this transfer.

The ip number used can be traced to a server in Iran, cf. Annex 4.

At the time when the incident was investigated by DK-CERT the server in Iran could not be identified as server providing anonymous services.

The legal department of 000domains informed me that Tucows was unwilling to voluntarily return the domain name to me, since the transfer request was initiated and approved by the admin contact email record in compliance with ICANN transfer policies. In a following dialog, 000domains' legal department informed me that Tucows was willing to return the domain to me if I signed an indemnification agreement. This did not seem like an attractive option to me.