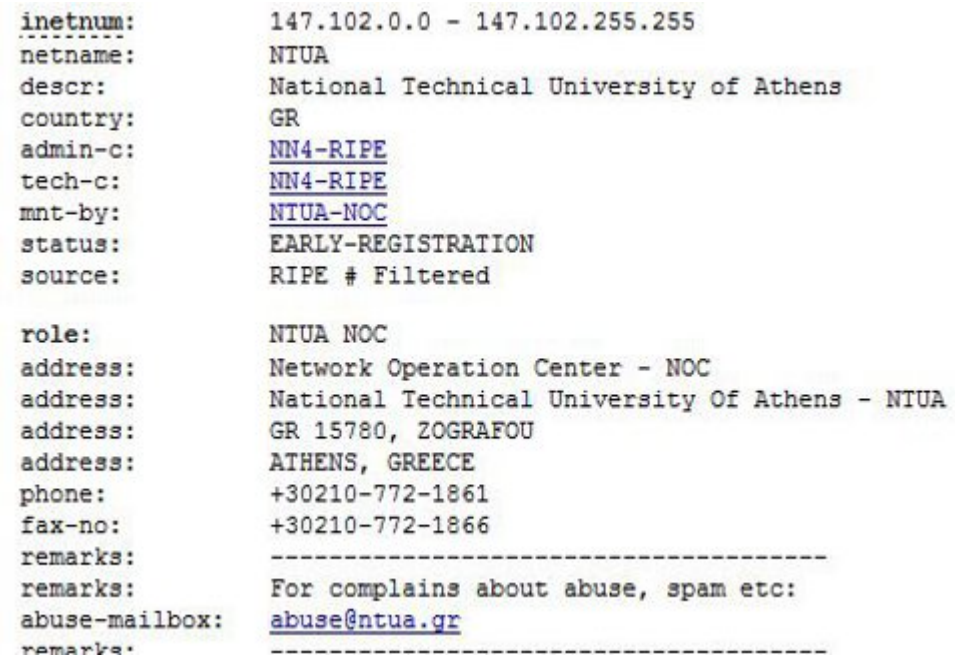
Geldwäscherei und verdächtige Aktivitäten



```
inetnum:        147.102.0.0 - 147.102.255.255
netname:        NTUA
descr:          National Technical University of Athens
country:        GR
admin-c:        NN4-RIPE
tech-c:         NN4-RIPE
mnt-by:         NTUA-NOC
status:         EARLY-REGISTRATION
source:         RIPE # Filtered

role:           NTUA NOC
address:        Network Operation Center - NOC
address:        National Technical University Of Athens - NTUA
address:        GR 15780, ZOGRAFOU
address:        ATHENS, GREECE
phone:          +30210-772-1861
fax-no:         +30210-772-1866
remarks:        ------------------------------------
remarks:        For complains about abuse, spam etc:
abuse-mailbox:  abuse@ntua.gr
remarks:        ------------------------------------
```

Sehr geehrter Kunde,

Als Teil unserer Maßnahmen zur Gefahrenabwehr, eine dringende Mitteilung / E-Mail wurde Ihnen von unserem Konto Abteilung POST BANK DE geschickt, um Ihnen mitteilen, dass wir nicht auf Ihre Post Bank Account Details in unserer Datenbank aufgrund von Geldwäsche-Aktivitäten überprüft wurden gefunden auf Ihrem Konto. Deshalb hat sich unser Finanzinstitut (Post Bank De) eine Null-Toleranz-Politik gegenüber Geldwäscherei und verdächtige Aktivitäten überwacht und sofort den Behörden zur Verfolgung resported

Aus Sicherheitsgründen haben wir vorübergehend gesperrt, bis Sie Ihr Konto wird unser sicheres Überprüfung abzuschließen.

Wie kann ich mein Post Bank-Konto zugreifen? Bitte folgen Sie den unten stehenden Link und aktualisieren Sie Ihre Kontodaten Genius Mittel zum Entsperren Ihres Genius Investing Konto für maximalen Schutz.
http://www.posbin-serve.co.cc/

Wir entschuldigen uns für die Ihnen entstandenen inconveninces haben könnte, dies ist Teil unserer Politik für unser Finanzinstitut und beachten Sie, dass unsere Bestätigungs-Prozess ist aus Sicherheitsgründen mit keinerlei Kosten.

Ich finde das gar nicht zum Lachen. Solche Phishing-Versuche würden nicht stattfinden, wenn nicht jemand darauf hereinfiele. Wie dumm muss man aber sein, um dann die Daten seines Postbank-Kontos einzugeben? Kann sich mal bitte jemand melden, der darauf hereingefallen ist und erklären, was er/sie dabei gedacht hat?

Übrigens steht im Quelltext der Phishing-Seite:
!– This site „www.posbin-serve.co.cc“ is using the free URL redirection service at http://freedns.afraid.org/ –
!– The real (cloaked URL) site can be found directly at http://www.top-alldevs.co.cc/enspave/login.php –
!– Please report any abuse of this free service –
Interessante Details dazu sind auch nicht schwer zu ermitteln.