„Phishing Domains“

and

nic.at

Richard Wein
nic.at

Content

- „Phishing-Domains“
- nic.at and Phishing
- Spamhaus.org
- Local Internet Community + Board

Background

- .at-domains were registered through registrars (most based in US) that
  - had no meaning itself (e.g. gifof.at)
  - with an existing Domainholder
  - were then used in URLs (e.g. http://www.bankofamerica.com.onlinebankingid99999999999999.gifof.at/session.cgi/
  - this URL led to a website that asked for bank details (maybe „Phishing Website“)

nic.at Involvement

- nic.at was contacted and requested to delete these domains
- nic.at reacted
  - by explaining the legal situation
  - by explaining the who-is-who, because doubts whether the „reporters“ understand the role of nic.at = REGISTRY and not a registrar
  - -> and did NOT withdraw the domains

Reasons for not-withdrawing

- not the domain is illegal
  - domain itself does not cause any harm
- not second level domain, but 5th, 6th, … SLD
  - not subject of contract between nic.at and domain holder
- potential fraud on website -> only content!
  - Austrian Supreme Court clearly states, that nic.at is not responsible for content on a website
- where to start and where to end with any illegal content (e.g. gambling, child pornography, …)
- nic.at should not take position of an „Internet Police“ or „Censorship Organisation“
- websites could be hacked (had various examples for that)

cause „Spamhaus.org“

- dispute with Spamhaus.org -> sent e-mail:
  - “incl. list of domains that should be removed because of being used for phishing”
  - “other Registrars and Registries regard the take-down of phishing domains as a high-priority obligation”
  - “threat to take action, which could have an adverse impact on our connectivity, if domains will stay active”

Reply from nic.at

- we do in no case support potentially illegal activities e.g. spam, phishing or other crimes
- explained reasons why we cannot withdraw a domain
- Solution: if we receive a proof of wrong domain holders data, we could withdraw domain according to our T&C

Reply: „Spam Block List“

- various IP-ranges of nic.at were put on Spam Block List from Spamhaus.org
- consequence: majority of e-mails could not be delivered to our Domainholders, Registrars and others
- nic.at formally requested IP-range to be deleted from list

Contacting Spamhaus.org

- help from other registries and external persons to get in contact with spamhaus.org
- talking to Richard Cox (CIO of Spamhaus)
- UK lawyer contacting spamhaus.org on behalf of nic.at demanding immediate deletion of the entry on Spam Block List
- finally all IP-ranges were taken from list, no further technical blocking of nic.at
- nic.at is still listed as a “Spam supporter” in SBL

LIC-Feedback

- broad support from public for our policy
- numerous positive articles in the press
- nevertheless discussion with Austrian LIC and our Board on future behaviour of nic.at as registry regarding SPAM / Phishing

Final Board Decision

- nic.at does definitely not support any illegal activities on the Internet
- we do not block or cancel any domains, if it does not violate our T&C
- we follow Austrian Law and Court decisions
- new: we will inform the relevant registrar and domain holder
- new: we forward necessary (hidden) information from our database to reporter of spam or phishing to help them
- new: domain-abuse@nic.at

Goals for ccNSO

- Discuss this issue with TLD community
- Work together with „Spam-fighting-organisations“
- Set up a „best practise“ paper
- ...???

Any questions ?

richard.wein@nic.at