Conficker Mitigation in .at

OARC Amsterdam 2009 Workshop

Otmar Lendl <lendl@cert.at>

I have two hats

The CERT.at Point of View

- As a national CERT we want to:
  - Protect our constituency
  - Protect others from being attacked from Austria
  - Reduce the amount of „badness“ in the Internet
- Thus:
  - Let‘s block those domains.
  - Use sinkhole data for warnings

The nic.at Point of View (1)

- We are a registry.
- We‘re in a quasi-monopoly position.
- We’re doing it for the country
  - The “land register” for the Austrian Internet
  - That the ccTLD is run by a private company is not a given.
- The only thing domain-holders get from us are NS records in the .at zone.

The nic.at Point of View (2)

- Our T&Cs only concern:
  - The domain itself must not infringe rights.
  - The owner information must be correct
- We don‘t care what people do with .at domains
  - We can‘t be the arbiter on what’s allowed on the Internet and what not.
  - If you have a complaint: Sue the owner.
  - If you want us to remove a domain, get a clear and valid order from a court.
- Past jurisdiction (and not just in Austria) supports this approach.

The nic.at conclusion:

- No action should be taken by the Registry.
- If we start to block domains because they might be used for something nefarious, we open a big can of worms.
  - Typosquatting
  - Phishing
  - Scams
  - …
- That was the plan as of March, 27th 2009

What did we end up with?

- AcoCERT (the CERT of the Austrian NREN) stepped up
  - Longstanding cooperation nic.at / Aconet / University of Vienna
  - “Conficker Research Project”
  - They run nameservers, sinkholes
- nic.at waived the registration fees
- We shared the sinkhole data
- NO change in the takedown procedures

Future

- This was an emergency
  - People tend to help each other in emergencies
  - Rules were bent
  - This is not the “war on terror”: we will declare this emergency to be over rather soon
- Avoid crying wolf too often
- Registries will revert to their previous stance
  - This is not the start of a new era
  - The next worm will likely be ignored by the registries