

Conficker Mitigation in .at

OARC Amsterdam 2009 Workshop

Otmar Lendl <lendl@cert.at>



I have two hats



- Leitbild
- Zuständigkeit
- Das Team
- RFC 2350
- Impressum

Leitbild

CERT.at ist das öst

Als solches ist CER

Bei Angriffen auf Re

Gesammelte Inform

Warum?

Weil IT Sicherheit e

Nur durch die Koor

The screenshot shows the nic.at website interface. At the top, there is a navigation bar with the nic.at logo and the text 'the austrian registry'. Below the logo, there are three main menu items: 'WHOIS / DOMAIN SUCHE', 'REGISTRIERUNG', and 'ÄNDERUNG'. The date and time 'Freitag 08. Mai 2009 | 13:46 MEZ' are displayed below the navigation bar. The main content area features two prominent buttons: a green one labeled '→ Domain Registrierung' and a grey one labeled '→ Domain Änderung'. The green button is highlighted and contains the text 'einfaches Registrieren' and 'Ihrer .at Wunschdomain' with a small map of Austria. To the right of the green button, there is a section titled 'Domain-Registrierung' with the text 'Sie sind nur einen kleine entfernt. Geben Sie einfa Suchfeld ein und klicken Bitte beachten Sie auch'. Below this text is a search input field with a green arrow button and the text 'www.' and 'IDN Eingabe'.

- 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

- 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.

- 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.

- 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

- 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

- 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