

Reducing DriveBy in .ch/.li

Cleaning .ch & .li Domains in a nutshell



SWITCH

Serving Swiss Universities

Bern, 10.11.11

Dr. Serge Droz
serge.droz@switch.ch

Motivation



- DriveBy infection are an issue for .ch
- Affected websites are **always** hacked
- As registry we know the domain owner and tech-contact
- A safe .ch is important for our business case
- There is a legal basis (AEFV 14f bis.)

Processes

Info about malware-domain

- Several Sources
- No active scanning

Confirm initial suspicion

- Tools assisted
- Final decision **always by human**

Inform domain owner

- By Mail to DO & TC
- Cc: Hoster
- **Give 1 Workday**

Suspend and inform agency

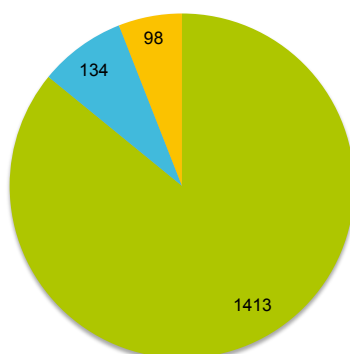
- Only if no reply
- At most for 5 days

One year and still going strong

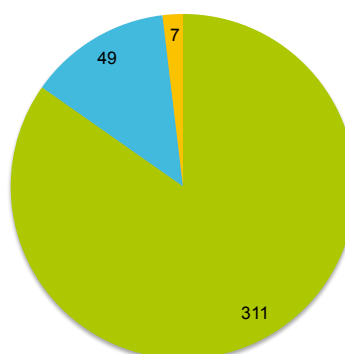
- Customer Feedback: Almost always positive



Domains processed



Since Start



Q3 2011

■ Cleaned without blocking

■ Cleaned after blocking

■ Not cleaned