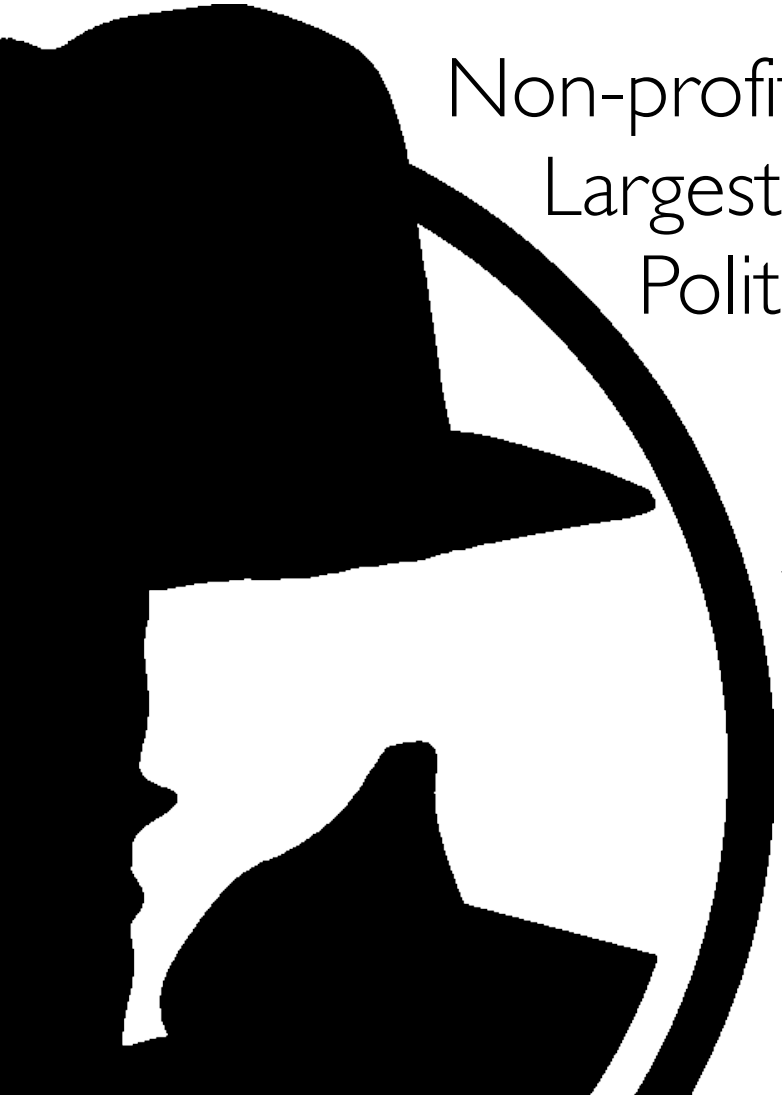
Introducing…
The Registrar of Last Resort

Benedict Addis
Shadowserver Foundation

About Shadowserver



Non-profit Internet security organisation

Largest victim notifier globally

Politically neutral

https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork

Registrar of Last Resort (RoLR)

RoLR: a special purpose registrar

Quarantine bad domains

- Spam
- Phishing
- Malware distribution
- Botnet command & control
- "Advanced Persistent Threat"

Limited scope

The problem

Malicious domain (2004)

Many malicious domains

EXAMPLE: CRYPTOLOCKER

1,000 possible domains/day auto-generated across seven TLDs
1st April 2014

. . .

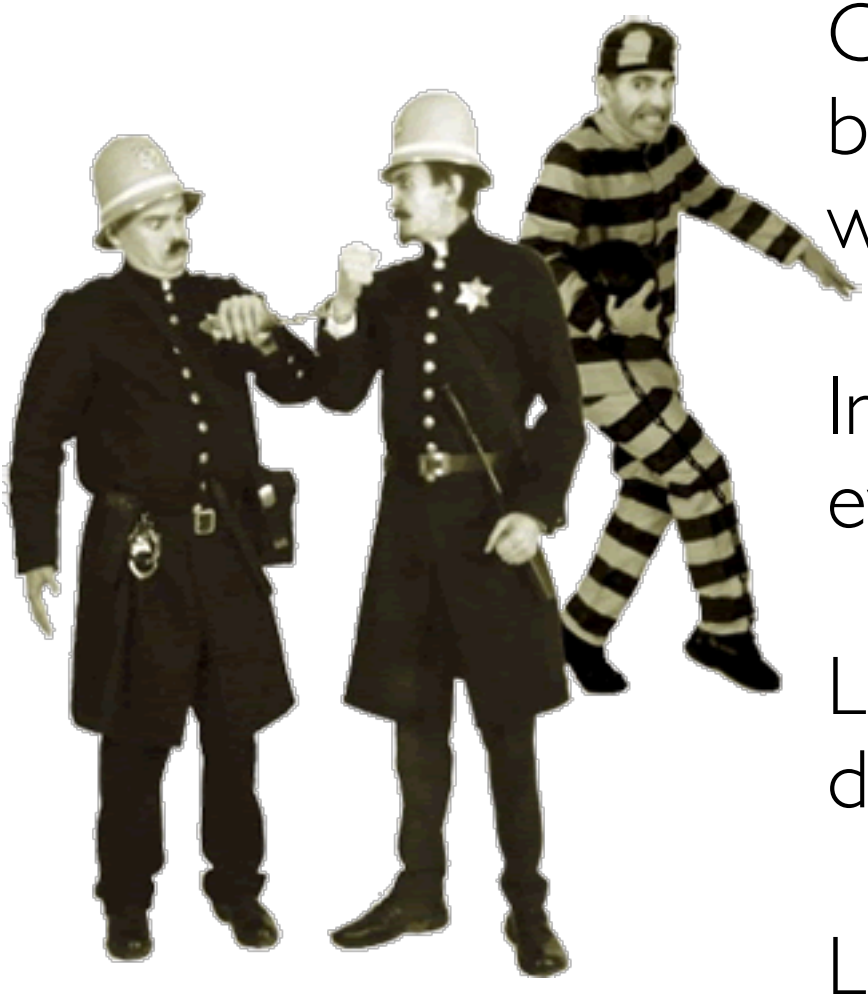
avyrwkqfybrxsy.com
natuwpmsqjecsm.net
aksgduuoktdyac.biz
nonjdaqcccpdqk.ru
cfdkwfiapjrvsd.org
pjxnwkenhreasx.co.uk
cgwaulfcrjrovc.info

Criminals exploit complexity

- Criminals shop for identifiers across registries, registrars, and jurisdictions
- Not necessarily motivated by cost
- Quick to identify and exploit weaknesses
- Create "asymmetry of forces"

The current response?

Public response



Court orders are slow, limited by jurisdiction … and not written by engineers

International co-operation is even slower - "MLAT problem"

LE response can be disproportionate

Little case law, less due process

Private response

Multiple competing companies with varying motives
Little accountability or transparency
Perverse incentives to not fix the problem
Doesn't scale

…but registries bear the cost

The registry acts as judge, jury and executioner for domain suspension

- Administrative costs
- Regulatory compliance
- Reputation of the registry
- Reputation of the industry
- Legal liability
- Ad-hoc process weakens ability to push back
- How to manage lifecycle of domains after suspension

Proposed solution

A trusted registrar

- Accepts transfer of existing domains
  - Under court order?
  - Notify registrant unless specifically prohibited / urgent need
- Registers un-delegated domains
- Securely manages portfolio of bad domains
  - Fail-safe model

Features

- Free at point of use
- Impartial, neutral, transparent and non-profit
  - Written constitution and narrow scope
  - Advisory committee to review acceptance criteria
  - Ethics committee to review abuse and complaints
  - Vetted contributors
  - Oversight by non-conflicted parties
- No special treatment required
  - Registrar complies with relevant law, contract and policies

Questions?

Benedict Addis
bee@rolr.eu