REMEDI3S-TLD: Reputation Metrics Design to Improve Intermediary Incentives for Security of TLDs

A project in collaboration with SIDN and NCSC

Maciej Korczyński
Delft University of Technology
Contact: maciej.korczynski@tudelft.nl

ICANN 54 Techday

19 October 2015, Dublin
REMEDI3S-TLD

Security incidents

DNS ecosystem
REMEDI3S-TLD

Security incidents
- SPAM
- Botnet C&C
- Malicious websites
- Phishing
- DNS amplification
- Fast-flux

DNS ecosystem
REMEDI3S-TLD

Security incidents
- SPAM
- Botnet C&C
- Malicious websites
- Phishing
- DNS amplification
- Fast-flux

DNS ecosystem
- Registries
- TLD
- Registrars
- Hosting providers
- Authoritative NS
- Resellers
Agenda

• Types of security metrics
• Security metrics for TLDs
• Security metrics for hosting providers
• Discussion
Types of security metrics

- Different layers of security metrics:
  - Top Level Domains (TLDs)
  - Market players related to the TLD (infrastructure providers): registrars, hosting providers, DNS service providers
  - Network resources managed by each of the players, such as resolvers, name servers
Security metrics for TLDs
Security metrics for TLDs

• Type of reputation metrics
  • Concentration of malicious content:
    a) Number of unique domains
    b) Number of FQDN
    c) Number of URLs
Security metrics for TLDs

• Type of reputation metrics
  • Concentration of malicious content:
    a) Number of unique domains
    b) Number of FQDN
    c) Number of URLs

• Size matters!
Security metrics for TLDs

- Type of reputation metrics (example)
Security metrics for TLDs

- Type of reputation metrics
  - Up-times of maliciously registered/compromised domains
Security metrics for hosting providers
Security metrics for hosting providers

1. Count badness per AS across different data sources
2. Normalize for the size of the AS (in 3 ways)
Security metrics for hosting providers

3. Rank ASes on amount of badness
4. Aggregate rankings
5. Identify ASes with consistently high concentrations of badness
Practical application

• “Clean Netherlands”: Enhance self cleansing ability of the Dutch hosting market by
  • promoting best practices and awareness
  • pressuring the rotten apples
Discussion

• Compare your TLD against the market
• Driving factors (why the attackers are more interested in certain types of domains?)
• Let us know about policy changes, pricing
Discussion

• Limitations: metrics for smaller TLDs are more sensitive to individual security incidents

• Abuse handling initiatives
Discussion

• Limited access to:
  • Domain WHOIS (classifier between maliciously registered and legitimate domains, metrics for registrars)
  • Datasets, e.g. shadow server reports

• Feedback
ACKNOWLEDGEMENTS

The research leading to these results was funded by SIDN (www.sidn.nl)

Many thanks to:

Cristian Hesselman (SIDN Labs),
Paul Vixie (Farsight Security),
and Thorsten Kraft (Cyscon)
Contact information:

Maciej Korczyński
Delft University of Technology
maciej.korczynski@tudelft.nl
Security metrics for TLDs

- Type of reputation metrics