Acronis

Domain abuse from the point of view of a ransomware protection company

Kevin Reed
kr@acronis.com
Share of malicious domains declines

Source: ICAAN DAAR report
Share of CnC and phishing domains grows
The fight with DGA

- Domain generation algorithms (DGA) allow attacker to have a new CnC domain often (typically – every day)
- There may be thousands valid CnC domains a day
- Sinkholing all of them is not practical or even possible
- They may be blocked at the recursive DNS server level, but
  - May be a significant investment
  - Does not scale
  - Complicated with DoH providers

- Should there be a process to delay DGA domains registration for a period of time?
The issue with registrars

- Fighting abuse contradicts registrars financial objectives
  - Less registrations, less money

- Registrars are not really motivated to keep DNS safe
  - They don’t operate the core infrastructure
  - They may operate authoritative DNS servers as paid or included option
  - … but they do have a separate AUP for them

- There are abuse resistant registrars
Acronis Foundation

Building a more knowledgeable future

CREATE, SPREAD AND PROTECT KNOWLEDGE WITH US!

Building new schools • Publishing books • Providing educational programs

www.acronis.org