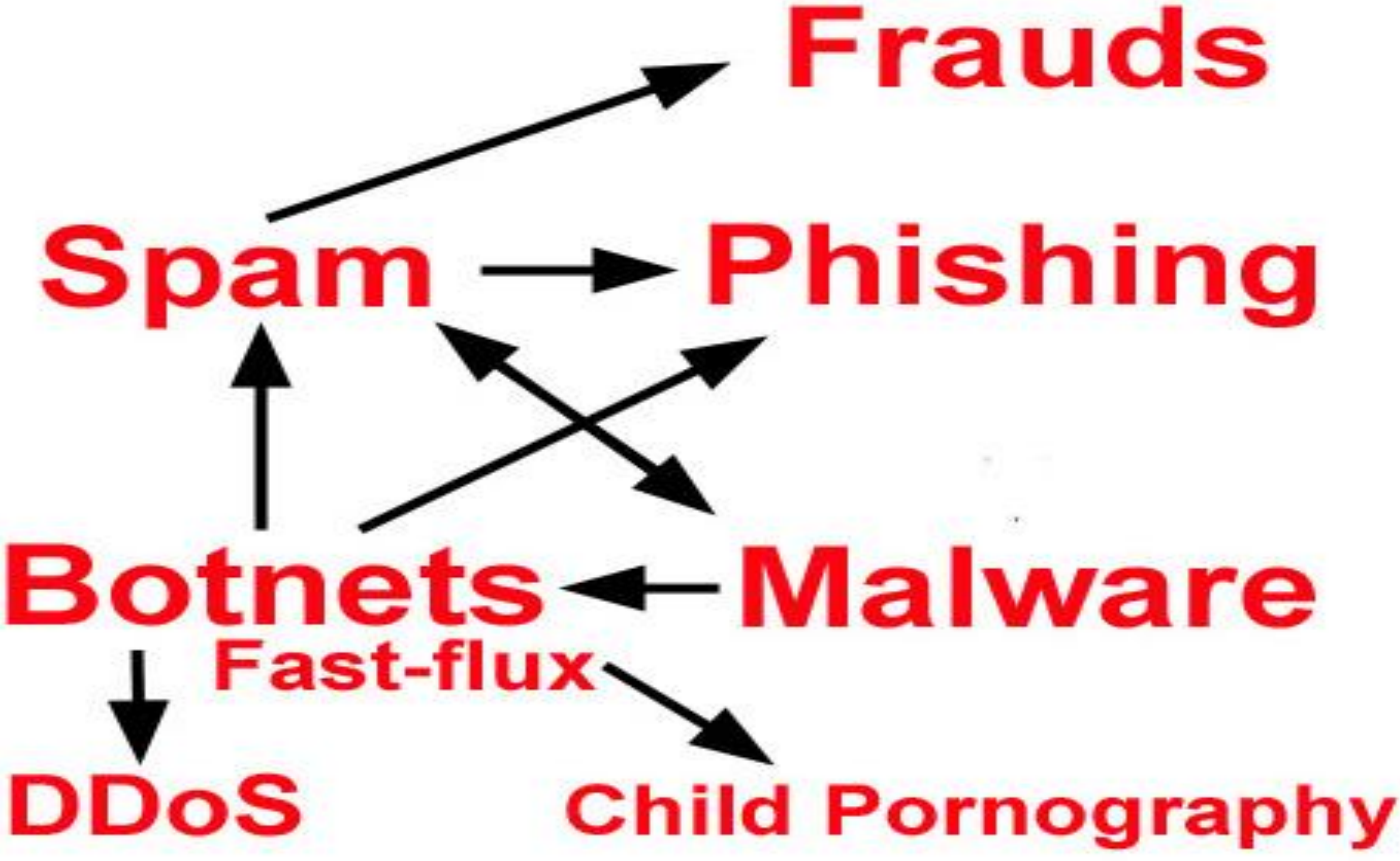
Take-Down or Block?

Ram Mohan
EVP & CTO
rmohan@afilias.info

DNS Abuse Forum
14 March 2011

The Interconnected e-Crime landscape



Frauds

Spam

Phishing

Botnets

Malware

Fast-flux

DDoS

Child Pornography

Take-Downs Can Work

- .INFO Anti-Abuse Policy into effect October 2009
- Registry is a central point for analysis and data dissemination
- Relationships with security community
- *Registry reports problems to registrar, so registrar can consider take-down*
  - Registrar has primary relationship with registrant, and can set and enforce its registrant contract
  - Registrars have superior data
  - Important to have good forensic proof of the abuse
  - Oct 2008 to March 2011: 563,000 .INFO domains have been reported to registrars
- Registry may act if necessary

Principles of Success

- Takedowns work because they address the problem at the source
- A takedown is a specific, direct response

DNS Blocking

- Blocking: not allowing queries to be fulfilled at some layer of the DNS. Different from suspending a domain by removing from the zone.
- It can be a disproportionate response to the problem.
  - Filtering e-mail at the organization level is a very effective way to control spam etc and protect your users.   But…
  - Virtually everything on the Internet depends on DNS
  - Web content, email, phone services, etc.
  - Blocking at the ISP or carrier level makes a decision for all customers – is that always the right thing? And mistakes are magnified.
  - Blocking TLDs is a slippery slope at the individual company level. Blocking TLDs at the ISP level or above could be disastrous.

DNS Blocking

- Creates confusion for Internet users because it’s difficult to understand who’s responsible and can correct the problem.
- Blocking is incompatible with DNSSEC
  - Blocking breaks the “chain of trust” and requires name servers to “lie”
  - DNSSEC interprets such lies as intrusion attempts
  - Undermines efforts to build trust in to the system, instead creating greater stability and security risks
- Once blocked, it can be difficult to recover or correct
- Beware collateral damage

Questions?

Ram Mohan
rmohan@afilias.info

DNS Abuse Forum
14 March 2011