Domain Abuse

A presentation to the ALAC

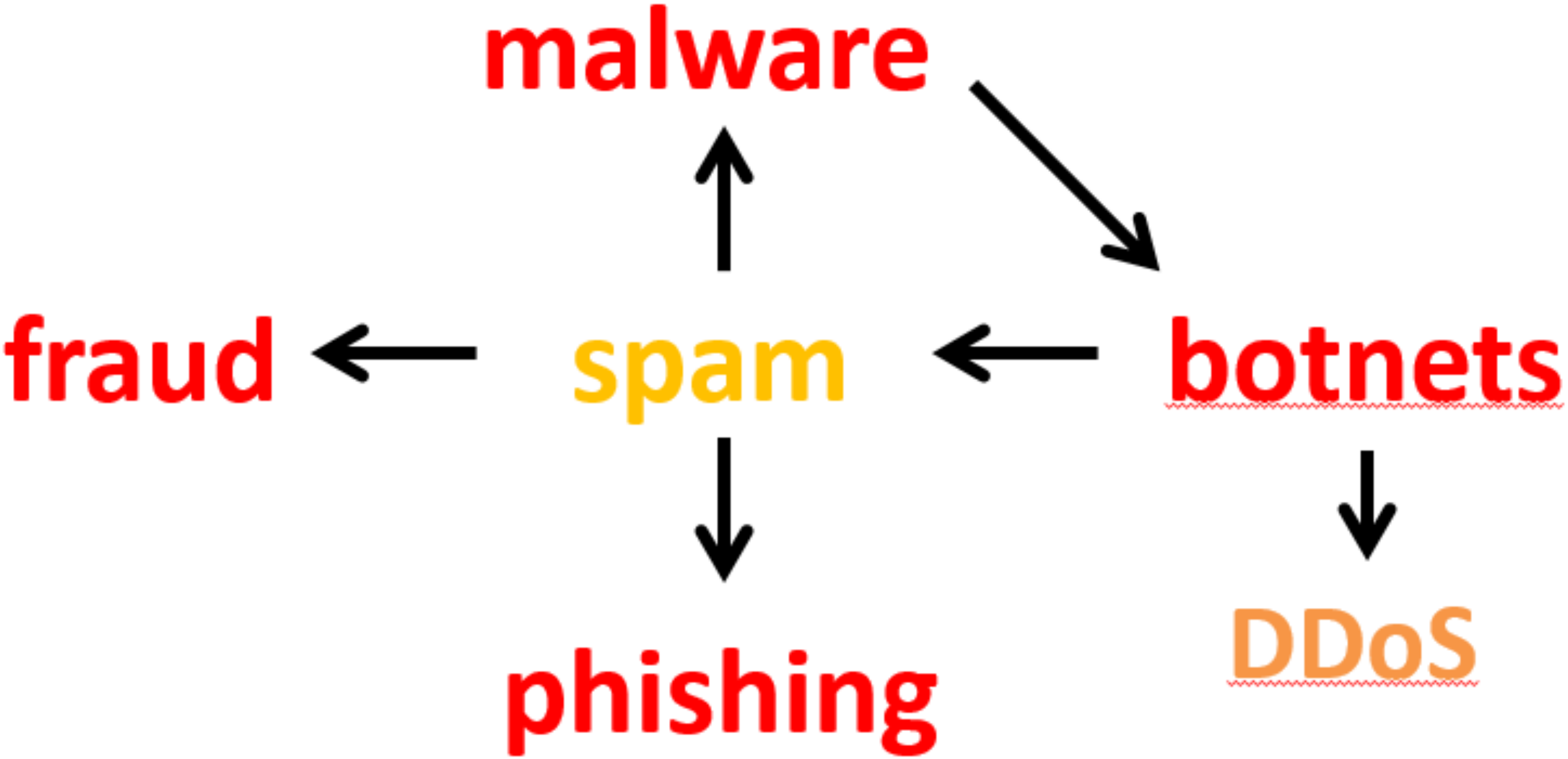
Greg Aaron

iThreat Cyber Group

28 June 2017

ICANN 59
POLICY FORUM
JOHANNESBURG
26–29 June 2017

Domain Abuse: Use of domain names to perpetrate harmful activities.



malware

fraud

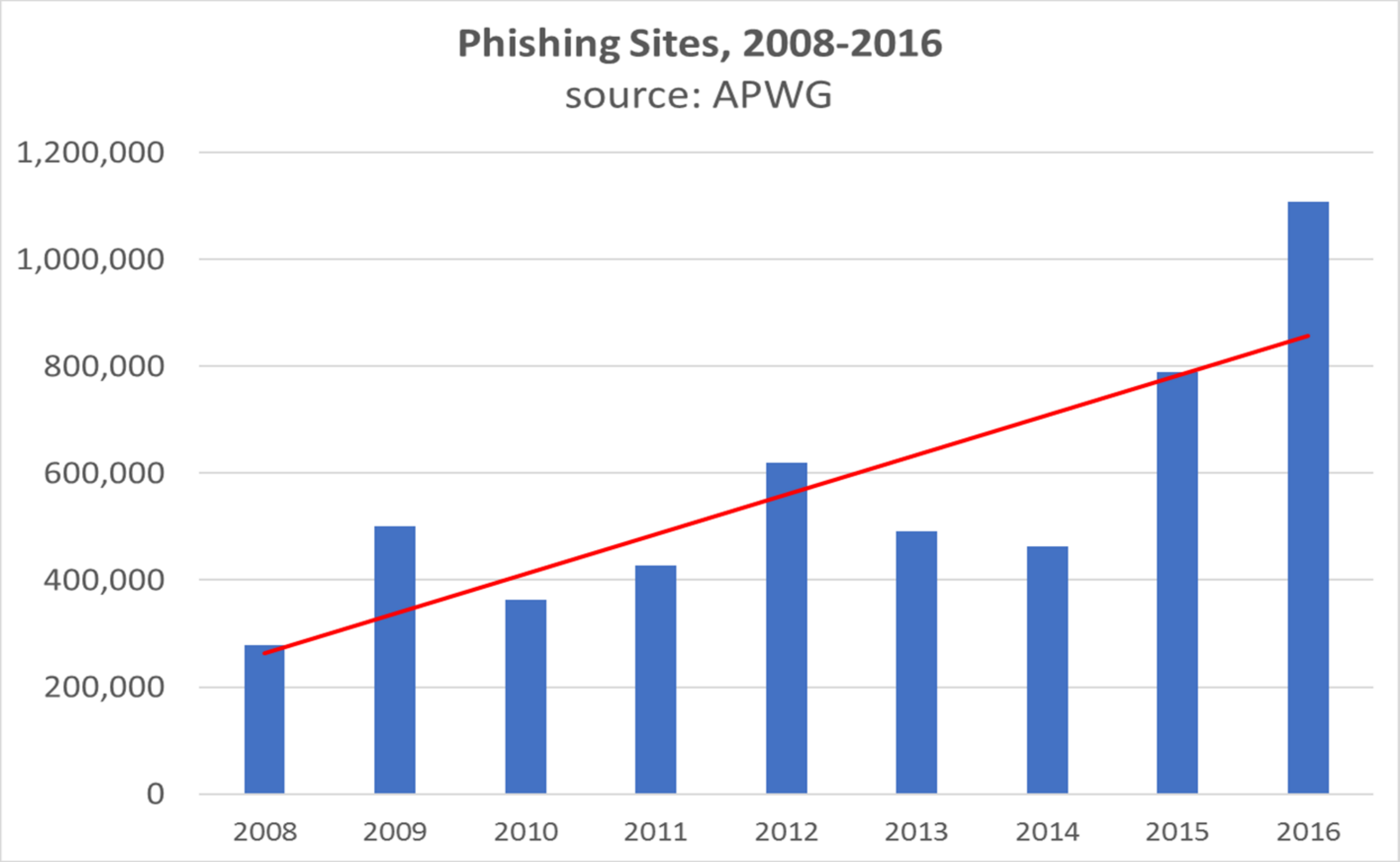
spam

botnets

phishing

DDoS

Phishing Attacks (and malicious domain use) up



ICANN 59 POLICY FORUM JOHANNESBURG 26–29 June 2017

Some Realities

- Cybercrime is more pervasive and more professional than ever.
- Abuse tends to concentrate in certain places, and moves over time:
  - Concentrations at certain registries (TLDs), registrars, hosting providers
  - Why? Inattention, low price, ineffective mitigation, or complicity.
  - Cases where service providers are operated for criminal purposes (Registrars: Estdomains, AB Systems, etc.)
- Mitigation is mainly done by private parties, not law enforcement.
  - On the Internet, relationships are governed by contracts.
  - The reach of any law enforcement body is limited by jurisdiction, and is necessarily slow.
  - Those who operate Internet resources have the responsibility to do so responsibly.
- Criminals know the domain system, and don’t play by the rules.

ICANN’s Role

- Bylaws: “The mission [of ICANN] is to ensure the stable and secure operation of the Internet's unique identifier systems” and policies “For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries”
- ICANN accredits registrars and registry operators.
- ICANN policies, placed in contracts via community input.
- Access to WHOIS data and zone files. WHOIS accuracy requirements (registrants, registrars)
- Prohibitions against malicious use of domain names (registrants)
- Anti-abuse monitoring, response, and reporting requirements (registries, registrars)
- ICANN’s contracts are enforceable.
- Suggestions: use those contractual tools to concentrate on the biggest, most harmful situations. Raise awareness of the problems.