Spam, Malware and Cybercrime

John R. Levine

CAUCE North America

CANTO August 2014

John.levine@cauce.org
Spam

- Fake drugs
- Porn
- One Million Dollars
- ...

Levine  CANTO  Aug 2014
Spam → Web

- Click on this link for ...
- Fake drugs
- Phishing
- Porn
- ...

Levine CANTO Aug 2014
Spam ➔ Web ➔ Malware

- Malicious or hacked site
- Installs malware
Phishing
Attacking your users

● Adware: shows annoying ads
  ● May replace legit ads

● Clickware: fake clicks
  ● “Man in Browser” clicks on ads

● Credential theft: online accounts
  ● Steal mail and web logins
  ● Send spam as your user
Attacking your users

- Credential theft: financial accounts
  - Steal banking credentials
  - Insert fake transactions with real ones
Botnets
Botnets

- Hijack computer to send spam
  - Provokes complaints
  - Wastes your bandwidth
  - Gets your network blocked
- Hijack computer for Denial of Service
  - Wastes a lot of bandwidth
  - May get you blocked
Botnets

- Hijack computer as malware host
  - Temporary or proxy web server
  - Wastes your bandwidth
  - Considered antisocial
- Hijack computer for other purposes
  - This month's special: Bitcoin mining
Countermeasures

- Stop outgoing spam
- Cooperate to detect and stop abuse
- Share data
- Build capacity
Outgoing spam

- Filtering
- Authentication

protected by SPF

DKIM.org

DMARC.org
Cooperation

- Best Current Practices
- Feedback loops
- Data providers
- Ad-hoc groups
- Trade associations
Best current practices (BCP)

- Port management
- Botnet mitigation
- Acceptable User Policies (AUP)
Feedback loops

- Tell senders about their spam
- User reports
- Spam traps
Data providers

- Spamhaus
  - Shares with trusted providers
- Specialists
  - Team Cymru
  - Return Path
  - Etc.
Ad-hoc groups

- Fight specific issues
- Trust-based Communities
  - Conficker Working Group
  - Torpig Working Group
  - Mariposa Working Group
  - DNS Changer Working Group
Public/Private initiatives

- Convened by FCC in the United States
- Mostly private members
- Recommendations not binding but persuasive
Intergovernmental groups

- London Action Plan
- ICPEN
- Interpol
CERTs

- Computer Emergency Response Team
- Generally national or regional
- Some public, some private
- Tend to have interesting meetings
Spam, Malware and Cybercrime

John R. Levine

CAUCE North America

CANTO August 2014

John.levine@cauce.org