Cooperation and self-regulation of Polish ISPs in combating online crime

Przemek Jaroszewski
NASK / CERT Polska
Agenda

- CERT Polska as a national CERT
- History of abuse forum in Poland
- Cooperation in practice
- Blackholing and filtering
- Challenges
Why CERT Polska?

- NASK is the registry for .pl
- CERT Polska was founded in 1996 (as CERT NASK)
- Early cases were mostly regarding networks of other Polish ISPs
- CERT Polska became a full member of FIRST in 1997, later joining other international forums

- Until today very few Polish CERTs and ISPs are internationally active
CERT Polska as a national CERT

- international activities + information sharing
- no hierarchy
- formal mandate: agreement with Polish Internal Security Agency and CERT.GOV.PL
• Communication done via email
• Limited response, hard to convince to cooperate
• Problem? We don’t know the people, they don’t know us
• Icebreaker over pizza and beer – it works but doesn’t scale 😊
Introducing the abuse-forum (2005)

- Let’s have one place for all to meet
- Who is all?
  - Large ISPs
  - The Police
  - CSPs
  - Other CERTs (military, government)
  - Mid-size ISPs
- Extensive and ongoing process
  - Cooperation with PLNOG
Cooperation with Law Enforcement

- helping to ask the right questions
- data retention
- working on data exchange interface
Data repository

- sharing operational information in a trusted manner
- infected hosts, phishing sites, botnets
- user certificates
- need-to-know policy
Blackholing concepts

BGP Blackholing – technology to block traffic directed to a given IP address at the level of (core) routers. BGP protocol is (ab)used to instruct routers to drop packets.

DNS Blackholing – technology to prevent from accessing certain domain names implemented on DNS servers. The servers return false data, either redirecting the user or stopping him.
BGP blackholing

- peering with about a dozen ISPs, including Polish Telecom (TPNET)
- /32 prefixes with bogons, host under DDoS, but also botnet controllers (!)
- the policy:
  - peers can inject hosts from own networks
  - NASK injects the bogons and controllers
  - anyone can choose to ignore parts of information (based on community numbers)
BGP blackholing – it took...

- 3 years
- a lot of trust to build
- legal challenges to fight
  - censorship?
  - limiting access to certain resources?
BGP blackholing – case studies

- TP decided to buy more sources of information
- gimp.org turned out to be co-hosted with an IRC server with several botnet-controlling channels
- Most of hate-mail was about one Polish soccer club fan page
BGP blackholing – summary

- it’s easy to implement (technically)
- it’s lightweight
- it’s arbitrary
Filtering port 25 tcp

- Initiated by TP, implemented on Dec 1, 2009
- Coordinated action with email providers, promoting switching to SUBMIT ports
- Very few problems encountered
- Effects
  - 99% reduction of spam from the service
  - 72% reduction of spam from TP overall
DNS blackholing

- Not implemented yet, but planned in NASK and TP in the nearest future

- Concept
  - Do it as an additional service benefiting the customers
  - Run on default nameservers

- Pros and cons
  - Less arbitrary than BGP blackholing
  - Requires more investments and communication towards users
Challenges with blackholing and filtering

- Transparency
- Legal obligations
- Legal limitations
- What should be filtered (botnet controllers, conficker domains, phishing domains, illegal content...)
  - Sources of information
  - Who takes the final decision?
I’m done, thank you!

- Questions?
- Comments?
CERT POLSKA

zgłoszanie incydentów: cert@cert.pl
strona internetowa: www.cert.pl
tel. +48 22 380 82 74
fax. +48 22 380 83 99

adres pocztowy:
NASK - CERT Polska
ul. Wąwozowa 18
02-786 Warszawa
Polska

DZIĘKUJEMY ZA UWAGĘ