Ukrainian Internet Crime
An International Perspective

Paul Vixie

Chairman and Chief Scientist

Internet Systems Consortium

UA-IGF, September 2011

Reputation Is Everything

- Internet is a loose federation of networks, most of which are privately owned and operated.
- There is no law, no law enforcement, no global authority who can ensure correct behaviour.
- Incorrect behaviour (spam, phish, malware, DDoS, etc) is not punishable in any direct way.
- Every network operator (worldwide) must take local measures to protect their security.
- This is done by reacting to *network reputation.*

Examples of Bad Behaviour

- *Spam*: unwanted push content (email, IM, blog comments). Has high cost to many recipients, low cost to a few senders. Violates economic assumption of the connecting parties ("equal value").
- *Phish*: credential theft by fake web sites advertised by spam. Stolen credentials later used to log into banking sites or to push more spam using first victim as a proxy.

More Bad Behaviour

- *Malware*: unwanted software installed without permission, usually as a result of a user visiting a web site that was advertised by spam. Used to create botnets for proxy access or DDoS.
- *DDoS*: distributed denial of service attack, to cause receipt of too much traffic, forcing a web site or other Internet service to go offline. Often done for hire and for ransom.
- These are just a few common examples, meant to inform this discussion without info overload.

Reputation As An Asset

- Internet criminals do not launch attacks from their own networks or using their own identities because they do not want their reputation to suffer and they do not want to be caught.
- Therefore they seek proxies whose reputations are previously unknown and thus presumed "good" by victims.
- The victim's only economical recourse is against the proxies, whose reputations then suffer.

Economics of Recourse

- It's not economical for every potential victim of electronic crime to maintain their own list of trusted network peers. (Gated community.)
- Therefore victims maintain (or subscribe to) lists of network peers having known-bad reputations (Black lists.)
- Total cost of operation depends on rate and cost of false positive vs. false negative events.
  - false positives are lost revenue (small), false negatives are added costs (large)

Examples of Cheap Recourse

- Much early use of new GTLDs was just spam
  - Some operators rejected all traffic from *.INFO
- Much use of distant CCTLD's is by spammers
  - Some operators reject all traffic from *.KR/CN/RU
- Most new 2LD/3LD domains are low value
  - Some operators reject all traffic from day-old names
- General assumptions of this kind are cheaper than investigating every event

Ukrainian Internet Crime

- A trivial and current example:
  - online-best-pharma.com.ua.
  - onlinebest-pharma.com.ua.
  - online-best-pharmacy.com.ua.
  - onlinebest-pharmacy.com.ua.
  - onlinebestpharmacy.com.ua.
  - online-buy-pharmacy.com.ua.
  - online-buypharmacy.com.ua.
  - onlinebuy-pharmacy.com.ua.
  - onlinebuypharmacy.com.ua.

Ukraine As A Proxy

- The hosting for the previous example comes from an ISP in Czech Republic.
- The distributors of the actual product are in Canada.
- The spammer was a freelancer, we think from Taiwan in this case.
- The ultimate victim in this case is Ukraine by damage to its reputation.

Some Implications

- It's not just domain names
  - Ukraine has at least one well known ISP whose primary business is hosting of e-crime services.
- Ukrainians are not always proxies
  - But when Ukrainian criminals operate online they use proxies outside Ukraine to hide their location
-

Ukraine Is Not Alone

- Every country is a target for this kind of reputation attack.
- Online criminals know exactly what country to target based on the strength of local law, policy, custom.
- The best defense is proactive: don't be the weakest or easiest country to use as a proxy.
  - Example: China and South Korea

Specific Recommendations

- Domain names under *.UA:
  - Residency requirement
  - Open and transparent "whois"
- Strong national CERT:
  - Clearinghouse for complaints about Ukraine
  - Educate Ukrainian ICT
- Lawful takedown:
  - Criminalize fraudulant or damaging activities even where the victims are outside of Ukraine

Summary

- Every country's economy now depends on the Internet and is affected by *network repuation*.
- Ukraine's image on the world stage today is as a weak proxy, friendly to Internet crime.
- Strong local laws and policies always cause criminals to move to an easier environment.
- This is a global problem requiring cooperation and action within every economy.