Crime

- An act committed or omitted in violation of a low forbidding or commanding it and for which punishment is imposed upon conviction

  http://www.thefreedictionary.com/crime
- Deviant behavior that violates prevailing norms --- cultural standards prescribing how humans ought to behave normally.

  http://en.wikipedia.org/wiki/Crime
- Is pornography against the law? Is it a crime? What about posting a syllabus from a course?
- http://www.cybercrime.gov/
- http://www.cybercrime.gov/cyberethics.htm

Cybercrime

- What is cyber-crime? Cyber-terrorism?
  - Hackers, Crackers, Warez, Malware, cyber-bullying, ..., Phrack, l0pht (old hacker)
  - Hacktivism
  - What's criminal, what's unethical, what's fun?
- Are online crimes virtual or real?
  - Is a website real? Does it exist?
  - Is bullying a crime?
  - Is stealing intellectual property like stealing a wallet?

Examples of Cybercrime

- Social engineering and hacking: Kevin Mitnick
  - Claims he didn't use technical tools
  - Markoff, Shimomura, solitary confinement
- SPAM: is this a crime? Why
  - http://tinyurl.com/6pkauo LA Times, 11/14/08
  - SPAM down two-thirds to 60 billion
  - Upstream ISPs cut off/de-peer McColo Corp
  - http://tinyurl.com/5bnpte MindMap

Srizbi stopped!

- We have observed that when a bot is unable to contact its hard coded control server, it will try to resolve the IP address of up to four domains. In our lab we have seen that a bot will then contact the server with this IP address and request a new template. Once a template is received it will begin spamming again: `gyprtwqy.com, faruoeqa.com, dqdpdrqq.com, syudwtqy.com`

  http://www.marshal.com/trace/traceitem.asp?article=816
- Why did this go on for so long?

Crime or FUD?

- If it has compromised your machine once, it will do it again. We've seen evidence" of this, says Roel Schouwenberg, senior virus researcher for Kaspersky Lab, which first discovered this new wave of Web attacks late last week.
- The SQL injection attacks, which appear to originate from China, appear to have peaked yesterday, according to Kaspersky. Among the infected sites found by Kaspersky were Travelocity.com, countyofventura.org, and missouri.edu.

http://ba.darkreading.com/security/attacks/showArticle.jhtml?articleID=212001872

Dark Reading continued

- Dan Hubbard, CTO at Websense, says the payloads vary, but many attacks appear designed to grab World of Warcraft credentials. "They do appear to have other capabilities, however, that allow them to update, disable AV, and...install more generic password stealers that could be used for a plethora of things."
- I stealing a WoW password like hacking your Wachovia account?

Cybercrime or Cybersomethingelse?

- http://www.youtube.com/watch?v=8_VYWefmy34
  - Kevin Mitnick on 60 minutes
- http://www.youtube.com/watch?v=J9hApKU1ZoQ
  - What's right and wrong with this CBC video?
- http://www.youtube.com/watch?v=-5zxOLZ5jXM
  - The new "face" of cybercrime
- http://sourceboston2008.blip.tv/file/770410/
  - L0pht participants reconvene

SPAM, Botnets, Making Money

- http://www.youtube.com/watch?v=anwy2MPT5RE
- http://www.youtube.com/watch?v=6wtfNE4z6a8

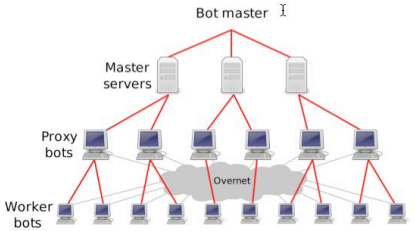


Figure 1: The Storm botnet hierarchy.

Spamalytics: Stefan Savage *et al*

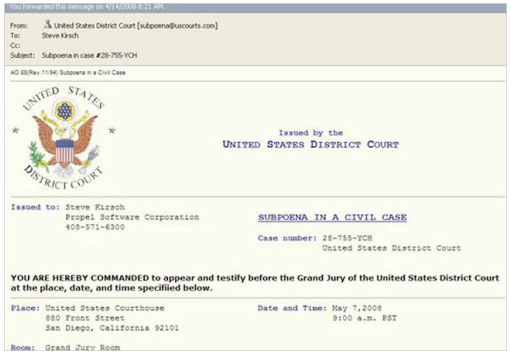
- …the only obvious way to extract this data is to build an e-commerce site, market it via spam, and then record the number of sales. Moreover, to capture the spammer's experience with full fidelity such a study must also mimic their use of illicit botnets for distributing e-mail and proxying user responses.
- In effect, the best way to measure spam is to be a spammer. In this paper, we have effectively conducted this study, though sidestepping the obvious legal and ethical problems associated with sending spam. Critically, our study makes use of an existing spamming botnet.

Phishing

- What is phishing, how does it work, origins
  - Email phishing attack
  - Web-based phishing attack
  - Certificate Authorities (CAs): a browser is what it says
  - User-interface and Human Factors issues
  - Tips on avoid being hooked
- There is a banking and financial crisis
  - Why is this a boon to phishing expeditions?
- Is this good advice? http://tinyurl.com/5dlr63

From Phishing to Whaling

- http://www.nytimes.com/2008/04/16/technology/16whale.html?fta=y



From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev. 11/94) Subpoena in a Civil Case

UNITED STATES DISTRICT COURT

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

Malware and Crimeware

http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf

- How is malware or crimeware distributed?
  - Web, email, hacking, worm
  - Social engineering: attachment, piggy-backing
  - (1) Distribute (2) Infect (3) Execute (4) Trouble
- DDOS, Spam, Click fraud, Data Ransom, ID theft
  - How can downloaded programs/code do this?
  - Why is Windows a more likely target?
  - What can you do to combat this threat?