Cybercrime, Cyberwar, Cyberterrorism

- In nuclear deterrence, both the Americans and the Soviets knew it was all or nothing: the Cuban missile crisis was resolved out of fear of catastrophic escalation. But in cyberattacks, the damage can range from the minor to the catastrophic, from slowing computer searches to bringing down a country’s cellphone networks, neutralizing its spy satellites, or crashing its electrical grid or its air traffic control systems.

http://nyti.ms/9k1w2i
JOHN MARKOFF, DAVID E. SANGER and THOM SHANKER

Cyber [War|Crime|Terrorism]

- bit.ly/tvg9yJ
  - Bully? Fighter? ...
- nyti.ms/uTO2rk
  - Iran, Siemens, ...
- bit.ly/sbGWGD
  - Anonymous? Attack?
  - No cyberwar exists
- 1.usa.gov/sTDNw2
  - Yes we can!
- zd.net/tm40Ce
  - WOW from China?

Crime and Cybercrime

- An act committed or omitted in violation of a law 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.

Cybercrime

- What is cyber-crime? Cyber-terrorism?
  - Hackers, Crackers, Warez, Malware, cyber-bullying, Blackhats, Whitehats, DDOS
- Cyberespionage, Cyber-sleuthing, Cyberwar
  - Imagined, real, over- or under-hyped?
- Hacktivism
  - Electronic civil disobedience?
- Criminal? Ethical? Enjoyable?
  - Why is the FBI involved in cybercrime?
Examples of Cybercrime

- Social engineering/hacking: Kevin Mitnick
  - Markoff, Shimomura, solitary confinement
- SPAM and Pornography
  - Are these crimes? Do they affect the Internet? Do they infect the Internet?
- Fake FDIC Phishing Scam
- Botnets, cyberwar, cyberespionage?
  - Is this really happening? Haxis of Evil?

Illegal, immoral, unethical

- Is pornography against the law? Is it a crime? What about posting a syllabus from a course, e.g., coursehero and other sites?
  - Other kinds of cyber activity/crime?
  - DOJ Kids and Internet Ethics
- Is sending SPAM against the law?
  - ftc CAN-SPAM

SPAM, Botnets, Making Money

- Original SPAM skit
- Ordering toast instead of SPAM

From worms to virii to botnets

- How do computers get “infected”?
  - Is the terminology warranted?
  - Trojan horse, attachment, host
  - Virus travels without human intervention
- When did this start? Personalities? Deeds?
  - Is there punishment? Too much/little?
**Robert Tappan Morris**
- **First Internet Worm**
  - Worm v Virus?
- **Valedictorian**
  - Delbarton, 1983
- **Computer Fraud/Abuse**
  - 1990, probation+$10K
- **Sold Viaweb to Yahoo for $48M in 1998**
- **Professor at MIT**
- **Father was Chief Scientist at NSA**

**DDOS: what and how**
- **Distributed Denial Of Service**
  - Terms? Mechanism
- **Misuse/abuse IP**
  - SYN, Ping, Smurf
- **Why do botnets help in this regard?**
- **IP addresses spoofed in SYN/Ping, why?**
- **Defensive measures against DDOS?**

**Reporting on Botnets**
BBC Click paid cybercrooks to buy botnet
Your licence fees at work
By John Leyden • Get more from this author
Posted in Spyware, 16th March 2009 12:32 GMT
Free whitepapers - Vulnerability management buyer's checklist
- **BBC buys a botnet!**
- **Aside from the legality of the scheme, the exercise raises troubling ethical questions. Security firms are almost unanimous in saying the behaviour of infected machines could have been illustrated without hacking into the machines of innocent victims**

**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, (discovered this new wave of Web attacks late last week.)
- 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.

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."
- Is stealing a WoW password like hacking your Wachovia account?

Cybercrime or Cybersomethingelse?
- YouTube Mitnick
  - Kevin Mitnick on 60 minutes
- YouTube on Cybercrime toolkit
  - What’s right/wrong with this CBC video?
- YouTube, new face of cybercrime?
  - The new “face” of cybercrime
- Hackers trailer
- See links at class links to cybercrime

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.
Spamalytics: Stefan Savage et al

- 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.

- National security threats by Internet Criminals

Phishing

- What is phishing, how does it work, origins
  - Email and Web phishing attacks
  - Certificate Authorities: site really is!
  - 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?


From Phishing to Whaling


Stuxnet

  - What was special about this worm, why a worm?
  - Origin? Destination?
  - Can we believe Wikipedia on this?

- How does attack unfold without Internet?
  - What is vector for spreading "disease"?
  - How does this work in practice?
  - Other issues?