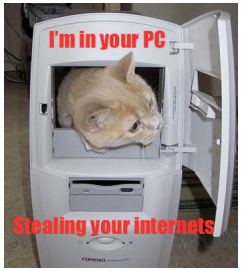
Crime and Cybercrime

- 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.

http://en.wikipedia.org/wiki/Crime

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: is this a crime? Why
  - McColo stopped, SPAM too! LA Times, 11/14/08
    - SPAM down two-thirds to 60 billion, McCol depeered
  - http://tinyurl.com/5bnpte MindMap from Washington Post
- 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?
  - http://www.cybercrime.gov/
  - DOJ Kids and Internet Ethics
- Is sending SPAM against the law?
  - ftc CAN-SPAM

SPAM, Botnets, Making Money

- Orignal SPAM skit
- Ordering toast instead of SPAM

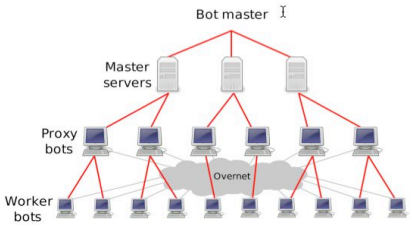


Figure 1: The Storm botnet hierarchy.

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 whitepaper – 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.

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."
- 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?
- Is this good advice? http://tinyurl.com/5dlr63

From Phishing to Whaling

- http://www.nytimes.com/2008/04/16/technology/16whale.html?fta=y
- http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf

You forwarded this message on 4/14/2008 8:21 AM.

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

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