(1988) "We're dealing with an urban myth. It's like the story of alligators in the sewers of New York. Everyone knows about them, but no one's ever seen them."

~Peter Norton on computer viruses

Of Norton Antivirus, Norton 360, Norton Internet Security, etc.
Notes

• Grades are updated for Homework and hands-on participation
• Bonus Homework & next week’s homework posted
  • (A two parter)
• This week the proposal is due
• Recitations (Today)
  • Discussion: Roberts 412
  • Hands on: Roberts 208
Review

Who is Assange?
A. Wikileaks founder  B. BBC News Anchor  C. New York Times Editor

Who was Thomas Drake?
A. New York Times Editor  B. Farmer  C. Whistle Blower
Viruses

*a piece of code that is capable of copying itself*

- **1959** – Victor Vysottsky, H. Douglas McIlroy and Robert P Morris (Bell Labs) - **Core Wars**
  - Game in which infectious programs named organisms competed with the processing time of PC
- **1966** – John von Neumann - **Theory of Self-Reproducing Automata**
- **1971** – Bob Thomas - **The Creeper**
  - Experimentally spread through ARPANET (The Advanced Research Projects Agency Network)
  - Self-Replicating Program
  - “I’m the creeper, catch me if you can!”
  - The Reaper was created to fix it
- **1974** – **Wabbit (Rabbit)**
- **1983** – Frederick Cohen - **“Virus” coined**
  - the computer programs that are infectious with a tendency to replicate
Worms

Worms spread from computer to computer with the capability to travel without any human action.

- **1988** – Robert Tappan Morris – **Morris Worm**
  - Cornell student Robert released 99 lines of code (from MIT) to try to assess how large the internet was
  - Because of bug, made several computers unusable
  - Contacted Harvard friend who tried to email instructions on how to stop or remove the problem
  - However the email could not go out because their virus had clogged the system
  - Estimated to have caused between $10,000,000 and $100,000,000 of damage
Worms

Worms spread from computer to computer with the capability to travel without any human action.

- **1999** – David L. Smith - **Melissa Virus**
  - ~20% of computers worldwide
  - Propagated to email first 50 contacts in Outlook with infected word document that contained a list of pornographic sites, The Melissa worm randomly inserted quotes from The Simpsons TV show into documents on the host computer and deleted critical Windows files.
    - Subject: Important Message From <name>
    - Here is that document you asked for ... don't show anyone else ;-)  

- Estimated to have caused $1 Billion Dollars in damages
- David was fined $5,000 and spent 20 months in jail
Worms

Worms spread from computer to computer with the capability to travel without any human action.

- **2000** – Reonel Ramones and Onel de Guzman in Phillipines – ILOVEYOU Virus
  - Emails with attachment LOVE-LETTER-FOR-YOU.TXT.vbs
- Ramones was kicked out of school after thesis denied
- Estimated to have caused between $5.5 - $8.7 billion in damages
- Charges were not brought against Ramones
- Spawned Movie “Subject: I Love You”
- [https://www.youtube.com/watch?v=Z3IP9mT6xxU](https://www.youtube.com/watch?v=Z3IP9mT6xxU)
Trojan Horses

Appear to be useful software, but like in the myth, conceal malware to your system. Unlike previous viruses, does not self replicate

• Used to create “botnets” or “zombie armies”, with which criminals can:
  • Send Their own spam or scams
  • Distributed Denial of Service (DDoS) Attacks
(Distributed) Denial of Service Attacks ([D]DoS)

*an attempt to make an online service unavailable by overwhelming it with traffic (from multiple sources)*

http://blog.lifars.com/2015/08/20/ddos-attacks-are-stronger-more-in-number-than-ever/
(Distributed) Denial of Service Attacks ([D]DoS)

an attempt to make an online service unavailable by overwhelming it with traffic (from multiple sources)

• Anonymous DDoS attacks on WikiLeaks “censors” Visa, MasterCard and PayPal
• Sony PlayStation Network DDoS
Phishing (Social Engineering)

- **Phishing**
  - “Fishing” for personal information
  - Misdirects users
  - Images on login pages are an attempt to fight things like phishing

- [http://www.it.cornell.edu/security/phishbowl.cfm](http://www.it.cornell.edu/security/phishbowl.cfm)
Phishing (Social Engineering)

[Image of a phishing email]

- **From:** <management@amazoncanada.ca>
- **To:** [email not shown]
- **Subject:** Suspension

**Dear Client,**

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to believe your account has been used by someone else. In order to prevent any fraudulent activity from occurring, we are required to open an investigation into this matter. We’ve locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:


Hovering over the link reveals it points to a non-Amazon site: "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013 Amazon.com, Inc. or its affiliates
Man in the Middle