We heard about the worm on 11/2/88


“On the evening of 2 November 1988, someone infected the Internet with a worm program. … This infection eventually spread to thousands of machines, and disrupted normal activities and Internet connectivity for many days.”
But there were ARPAnet attacks in 1986


“The hacker’s code name was “Hunter” – a mystery invader hiding inside a twisting electronic labyrinth, breaking into U.S. computer systems and stealing sensitive military and security information”
Hackers were once a nuisance

Source: Time Magazine, December 12, 1994

- Newsday technology writer & hacker critic found:
  - Email box jammed with thousands of messages
  - Phone reprogrammed to an out of state number where callers heard an obscenity loaded recorded message

Other nuisance activities

- Free use of computing cycles, storage, networks
- Avoiding phone charges
- Technical “explorations” by the curious
- “noisy” viruses that clogged our mail boxes
Then it got more serious


An international group attacked major companies: MCI WorldCom, Sprint, AT&T, and Equifax credit reporters.

• Had phone numbers of celebrities (e.g. Madonna)
• Had access to FBI's national crime database.
• Gained information on phones tapped by FBI & DEA
• Created phone numbers for their own use
Russian hacker accessed Citibank computers and transferred $10M to his accounts using passwords and codes stolen from Citibank customers

- Citibank & FBI tracked Levin
- all but $400,000 recovered
DDOS attacks become a reality

Source: Seattle Post-Intelligencer Staff and News Services; February 9, 2000

- Operations of major e-commerce & web sites seriously disrupted
  - Amazon.com, eBay, CNN, others

DDOS attacks continue to be a significant problem

- Attacks against competitors sites
- Extortion attempts
- Political statements (e.g. Estonia)
Links made with organized crime

Source: Ecommerce Times – March 9, 2001

FBI advises that Eastern European hacker groups stole information from e-commerce & online banking sites

- 40 firms in 20 states, lost over 1M credit card numbers
- credit card information sold to organized crime entities.
- the criminal groups usually try to sell security services to victim sites
The relationships grow


Easter European Internet sites traffic in tens of thousands of stolen credit-card numbers weekly

- Claims financial loses of over $1B/year
- Cards prices at $.40 to $5.00/card – bulk rates for lots of hundreds or thousands
- Organized crime groups buying from black-hat hackers
Spyware Targets Individuals

Source: The Register, Aug 30 2002

Spyware freely available

- Distributed via email
- Logs keystrokes and copies all email
- Sends recorded information to a specified email address
Extortion


- Oleg Zezev, a/k/a "Alex," a Kazakhstan citizen, sentenced to 51 months in prison following his conviction on extortion and computer hacking charges.
- Convicted of hacking into Bloomberg L.P.'s computer system; stealing confidential information and threatening public disclosure if $200,000 not paid.
The Rise of the Cyber-Mercenary

BotNets for hire

• Source: Technology Review - September 24, 2004
  — Rent pirated computers for $100/hour
  — Average rate in underground markets
  — Used for sending SPAM, launching DDOS attacks, distributing Pornography, etc..

Other services available as well

• Custom attack tools, viruses, worms – guaranteed to go undetected by common anti-virus products
• Data thieves for hire
Going “phishing”

Definition

• Phishing: fraudulent email and websites used to lure recipients into divulging sensitive information such as credit card numbers, social security numbers, bank account numbers & PINs, etc.

A rapidly growing problem

• Anti phishing working group (www.antiphishing.org)
  — Dec. 03 – reports increase 400% over holidays
  — Feb. 04 – reports increase 50% in January
  — March 04 – reports increase 60% in February
  — April 04 – reports increase 43% in March
  — May 04 – reports increase 180% in April
  — Jan 05 – 300% increase over May 04
Identity theft flourishes (1)

- Chronicle, October 21, 2004 – reports on theft of Social Security numbers from UC Berkeley systems; 600,000 Californians affected
- Associated Press, November 4, 2004 – reports a former University of Texas student indicted on hacking into UT’s system and stealing Social Security numbers and other personal information from more than 37,000 students and employees.
- Los Angeles Times, November 4, 2004 – reports four computers stolen from Wells Fargo; lost Social Security numbers of customers
- Computerworld, January 10, 2005 – reports hacker steals names, photos and Social Security numbers of more than 32,000 students and staff at George Mason University
- news.com, Feb 15, 2005 – reports ChoicePoint confirmed that criminals accessed its database of consumer records, potentially viewing the data of about 35,000 Californians; at least one case of identity fraud
A growing electronic crime infrastructure

Source: Baseline Mag, March 7, 2005

• Web mobs named carderplanet, stealthdivision, darkprofits and the shadowcrew
  — Buy and sell millions of credit card numbers, social security numbers and identification documents
  — Often for less than $10 each
  — Build sites and services to create more skilled, like-minded organizations.

• U.S. Secret Service said Shadowcrew had 4,000 members
  — Sold 1.5 million credit card numbers, 18 million e-mail account and other ID documents
  — Sold to highest bidders
With links to terrorist activities

Source: Testimony of Mr. Dennis Lormel, FBI; Senate Subcommittee on Technology, Terrorism and Government Information - July 9, 2002

- Terrorists have used identity theft & Social Security Number fraud to obtain employment and access to secure locations.
- Also used by terrorists to obtain Driver's Licenses, bank and credit card accounts through which terrorism financing is facilitated.
- Terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell.
Pentagon Computers Breached

Source: GovernmentExecutive.com: March 5, 2008

“Defense Officials still concerned about data lost in 2007 network attack”

• For a period of two months starting in June 2007 an “amazing amount of data” was stolen from an unspecified number of Pentagon Computers
Defense Industrial Base Attacked

Source: Wall Street Journal, April 21, 2009

“Computer Spies Breach Fighter Jet Project”

- Networks of defense contractors breached and terabytes of data related to designs and electronics of the Joint Strike Fighter siphoned off
Cyber-war?


"The United States is fighting a cyber-war today, and we are losing. It's that simple," warned Mike McConnell, President Bush's Director of National Intelligence"