Worms, viruses, etc.

Guevara Noubir
Northeastern University

Malware

- Computer systems still have many vulnerabilities
  - When exposed to the Internet leads to exploitation
  - Major issue as computer systems become more ubiquitous
- Malware is a generic term that refers to malicious software
- Terminology
  - Virus: computer program designed to spread (require human intervention)
  - Worm: does not require human intervention
  - Trojan horse: allows remote access to unauthorized users
  - Adware: ads when application is running
  - Spyware: monitors & collets information to be transmitted to a third party without user knowledge/consent

Why?

- Controlling millions of Internet hosts is feasible
- DDoS and blackmailing
- Access information
  - Passwords, credit cards, email accounts
- Computation/search
  - Cracking keys
- Confusion
- Cyber warfare, terrorism, etc.

History (1971 -)

- Worms self-replicate by exploiting vulnerabilities in remote machines
  - Apps running on some port
  - Vulnerabilities are purchased for malicious and legitimate use (e.g., CISCO)
- Worms carry a payload to take actions

- One of the first worms to extensively spread by Robert Morris, 1988
  - Uses fingerd and sendmail buffer overflow, rsh, weak passwords
  - Around 10% Internet hosts infected
  - Convicted, 3 years of probation, 400 hours of community service work

- Many worms since then with a peak during 2000-2004 period
- Today worms are more stealthy

Code Red CRv1

- "How to Own the Internet on your Spare Time", S. Staniford, V. Paxson, N. Weaver, USENIX Security 2002.

- Date July 13th, 2001
- Exploit
  - Microsoft IIS webservers using .ida vulnerability [published June 18, 2001]
- Payload
  - Website defacement
- Spreading
  - 99 threads: each generates random IP address and infects
  - 100th thread: defaces website
- CRv1 had a bug in RNG
  - All copies of thread had the same sequence rng(seed, thread identifier), no-current-host-IP => linear spread

Code Red CRv2 or Code Red I

- Date July 19th, 2001
- Fixed bug in CRv1 and changed payload to DDoS www.whitehouse.gov
- Analysis:
  - N: vulnerable nodes (no patching during propagation time)
  - k: (constant) number of vulnerable hosts which can be found and infected in an hour at the start of the incident by one infected machine
  - a: proportion of vulnerable machines compromised
  - t: time
  - Nda/dt = Nak(1-a)

- Gives a good prediction model

Code Red II

- Date August 4, 2001
- Exploit: another MS IIS buffer overflow
- Installed a root backdoor allowing unrestricted remote access
- Spreading (pretty successful): probability based
  - 3/8 => random class B address
  - 1/2 => random class A address
  - 1/8 => whole Internet

Nimda

- Date September 18th, 2001
- Exploit: multi-vector (few minutes – 22 minutes)
  - Yet another MS IIS vulnerability
  - Email attachment
  - Copies across network shares
  - Adds exploit code to webpages
  - Scans for backdoors of Code Red II, sadmind
- Payload unknown
  - The worm has a copyright text string that is never displayed: (From F-Secure)

    "Concept Virus(CV) V.5, Copyright(C)2001 R.P.China"

More Advanced Techniques

- Hit-list scanning
  - Start with 10K-50K potential targets; divisions with each generation => few seconds to cover hit list
  - Preparing hit list: stealthy scans, distributed scans using 10s – 1000s zombies, dns search, spiders (web crawling), listening (infected machines spread and reveal that they are vulnerable)
- Permutation scanning to avoid multiple probes
  - Use secret key to permute IP address space
  - Scan permuted space sequentially
  - When an already infected host is detected randomly jump
- Hit-list + permutation scanning => warmhol estimated to infects most vulnerable targets in ~15 minutes (300,000 vulnerable machines out of 2^{32})

Other Worms

- MS SQL Slammer
  - Date January 25, 2003
  - Buffer overflow in MS SQL Server
  - Doubled every 8.5 seconds until network collapse
  - 90% of vulnerable hosts infected in 10 minutes (75,000)
- Check
  - http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms

- Where did all the worms go?
  - More stealthy, instrumentalised for financial benefits, cyber-crime, targetted attacks
  - Conficker A, B, C, D, E: since November 2008 infected 9-15 million hosts
  - In 2009, Panda Security analyzed 2M machines and found 6% infected

Stuxnet

- Stuxnet is a computer worm with unique characteristics
- Targets specific SCADA systems
  - Supervisory Control and Data Acquisition systems
  - Control industrial systems such as power plants
- Stuxnets spreads slowly searching for specific SCADA systems and reprograms their PLC

How does it operate?

- Stuxnet uses 4 zero-day attacks as infection vectors + other bugs
  - USB drive, print spooler, two elevation of privilege bugs
- Spreads slowly (to max three nodes)
- When spreading over the network remains local to the company
- Looks for a windows machine with
  - WinCC/PCS 7 Siemens Software that controls PLC
  - Checks for Variable Frequency Drives (AC rotational speed controllers)
  - Focuses on two vendors (Vacon & Fararo Paya)
  - Attacks systems that run between 807-1210Hz
  - Modifies the output frequency for a short interval of time to 1410Hz and then to 2Hz and then to 1064Hz
- Tries default passwords
- Hides existence by installing malicious drivers signed using two stolen keys (Realtek, JMicron)
- 60% damage believed to be in Iran

Remarks

- Security is about the whole system
- Software vulnerabilities are still a major issue
- Public Key Infrastructure and deployment is weak
- Network architecture not designed with sufficient security
- Human factor, users, passwords, policies
- SCADA system are vulnerable and critical