Foundations of Network and Computer Security

John Black

Lecture #11
Sep 28th 2004

CSCI 6268/TLEN 5831, Fall 2004

Announcements

- Quiz #2 today
- Please sign a disclaimer if you have not already done so
  - I have them with me
- Project #0 due a week from today
  - Please hand in on paper in class
  - Distance students can email directly to Mazdak
- Project #1 has been assigned

Network Security: The Biggest Challenges

- What are the biggest problems now, today, on the Internet
  - What are the most common types of attacks?
    - Viruses, worms
    - Break-ins via software vulnerabilities
    - Denial of Service attacks (DoS)
      - And Distributes Denial of Service (DDoS)
  - What about keyloggers, spyware, rootkits?
    - Not as relevant to network security
    - More likely to be end-results of other break-ins
      - A recent virus was found to install a keylogger

Viruses (Worms)

- Today, most everyone just calls them viruses
  - Technically most are “worms”
  - Worm is a self-contained propagating program
  - Viruses embed in other programs and self-replicate
    - Kind of like viruses in biology

Viruses: History

- Morris Worm, Nov 2nd, 1988
  - The first worm (I know of) was the Morris worm
  - Robert T. Morris, Jr.
    - 23 years old
    - Cornell grad student
    - Father worked at the NSA (whoops!)
  - Wrote a self-propagating program as a “test concept”
    - Exploited Unix vulnerabilities in sendmail and fingerd
    - Released at MIT
    - Bug in the worm caused it to go wild
      - Probably wouldn’t have caused much damage otherwise!

Morris Worm (cont)

- Shut down thousands of Unix hosts
  - But this was 1988…
- Reactions
  - People didn't know what to do, so they panicked
    - Disconnected from net
    - Unable to receive patches!
  - Morris fined $10k, 3 yrs probation, 400 hrs community service
  - CERT was created

CERT -- They were first

- Carnegie mellon Ermergency Response Team
  - But don’t expand it into an acronym
- Provide technical advice and coordinate responses to security compromises
- Identify trends in intruder activity
- Work with other security experts to identify solutions to security problems
- Disseminate information to the broad community
- Analyze product vulnerabilities
- Publishes technical documents
- Presents training courses

Modern Viruses

- Almost all look for Windows hosts
  - Windows runs on more than 90% of desktops these days
  - A lot of hosts on cable modems
    - Fast, always on
  - Destructive payloads
    - Wipe hard disk, eg
    - Some install backdoors for later use
  - All kinds of weird behaviors though
    - Some innocuous

Viruses: Why?

- Who writes these things?
  - Typical profile: male, teenager, geeky, smart
  - Script Kiddies
    - Don’t really write them, but launch them
    - Sometimes make small mods and call them their own
    - Scariest hackers: beyond the reach of the law
- Why?
  - Intellectual challenge (sigh…)
  - Peer recognition
  - Bot building (Zombie armies)
  - Because it’s there?

Brief History

- Would take weeks to look at all the viruses we've seen
  - Also, wouldn't be *that* instructive
- We'll look at the ones I think were most instructive, important, and which have interesting lessons
  - So it's a *selective* brief history of viruses

AIDS Trojan (1989)

- Often called a “virus”
  - A trojan is a program with a “surprise” payload
  - The AIDS trojan was distributed as a way to enable graphics on TTL monitors
    - Duh
  - Payload: erase harddisk

- Interesting note: first virus scanners appear around this time (1990)

Tequila (1990)

- First polymorphic virus
  - Polymorphic means “changing form”
  - This was done to defeat virus checkers
- Current status (2004) of polymorphic viruses
  - Well, the current virus toolkits (MPC, VCS, VCL) create code which is still caught by scanners
    - VCL – Virus Creation Laboratory (1992); pull-down menus, selectable payload
  - But it’s possible to make a toolkit which will defeat the scanners – hasn’t been done yet

Michelangelo (1992)

- First virus to get lots of headlines
  - Lives in MBR (master boot record)
  - Targets MS-DOS machines
  - Transfers to floppies/hard-disks when intermixed
    - Note this predates widespread use of the Internet
  - Payload: destroy boot and FAT on March 6th
    - Michelangelo's birthday

DMV (1995)

- Word Macro virus
  - Macros are sets of executable instructions specific to an application
  - Back in 1995, MS Word was configured out-of-the-box to execute immediately any macros in a Word document
  - This meant that simply opening a document in an email or from the Web was dangerous
- DMV
  - Distributed with the paper “Document Macro Viruses”
  - Harmless (even had dialog boxes)
  - Trying to prove a point
- Other macro viruses possible with Excel, Access, Adobe Acrobat, and more

Back Orifice Trojan (1998)

- Pun on MS Back Office
  - Allows remote access via the Internet of Win 95/98 boxes (BO-2000 runs on Win 2k and NT)
  - Waits for commands starting with "*!*QWTY?"
    - US version used encryption; international could not! ☺
  - Doesn't show up in the task list
  - Written by cDc (Cult of the Dead Cow) and advertised as a legitimate tool
    - Used by network managers, in fact
  - But has been abused of course
    - Has plug-ins to 0wn your box (view remote screen, download registry, etc)

Melissa (1999)

- Just when you thought it was safe
  - Melissa was a major virus
  - Combination Word Macro virus and email virus
    - Sent as an attached doc file
    - Scanned Outlook address book and sent itself to first 50 addresses
    - Subject: “Important message from <you>”
    - Body: Here is the document you asked for; don’t show anyone
      - Then attached the most recent doc you had been working on, infected with Melissa
    - Spread VERY rapidly all over the world
      - Tons of variants

ILoveYou (2000)

- Clever technology, great social engineering
  - Subject: I love you
  - Body: Kindly check attached love letter from me
    - And message was from sender you know!
  - Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs
    - Note the double-extension – VBS script
    - If you didn't have your OS set to show extensions, you'd just see LOVE-LETTER-FOR-YOU.TXT

ILoveYou (cont)

- Complex payload
  - The worm copies itself into two places where it will be executed on each computer restart.
  - It will try to send itself to every entry in your Outlook address book.
  - The worm searches all drives (local and networked) for files ending in VBS, VBE, JS, JSE, CSS, WSH, SCT or HTA. If found, they are overwritten with the virus and their extension renamed to .VBS.
  - Graphics file with JPG or JPEG extensions are also overwritten with the virus and .VBS added to their name (so they will end up with a double extension).
  - Multimedia files with MP2 and MP3 extensions are marked as hidden and then copied to a new file with the same name and .VBS added. (Note that of all the files attacked, these are the only ones that can be recovered directly; all others have to be recovered from backups.)

ILoveYou (cont)

- Was wildly successful
  - Mostly due to human nature: someone loves me
- Has countless variants
  - Joke attached
  - Mother's Day Gift confirmation
    - Now that's just wrong
  - How to stop the ILoveYou virus

It Gets Worse

- SirCam, Nimda, CodeRed, BadTrans
  - Nimda: very complex
    - Mostly spread via unpatched IIS servers, but also
      - Via email (attached EXE)
      - Browsing dubious web sites with unsecured browser
      - Using backdoors from other viruses (CodeRed II, eg)
      - Payload: back door access
  - Code Red: still around today!

Stealth Viruses