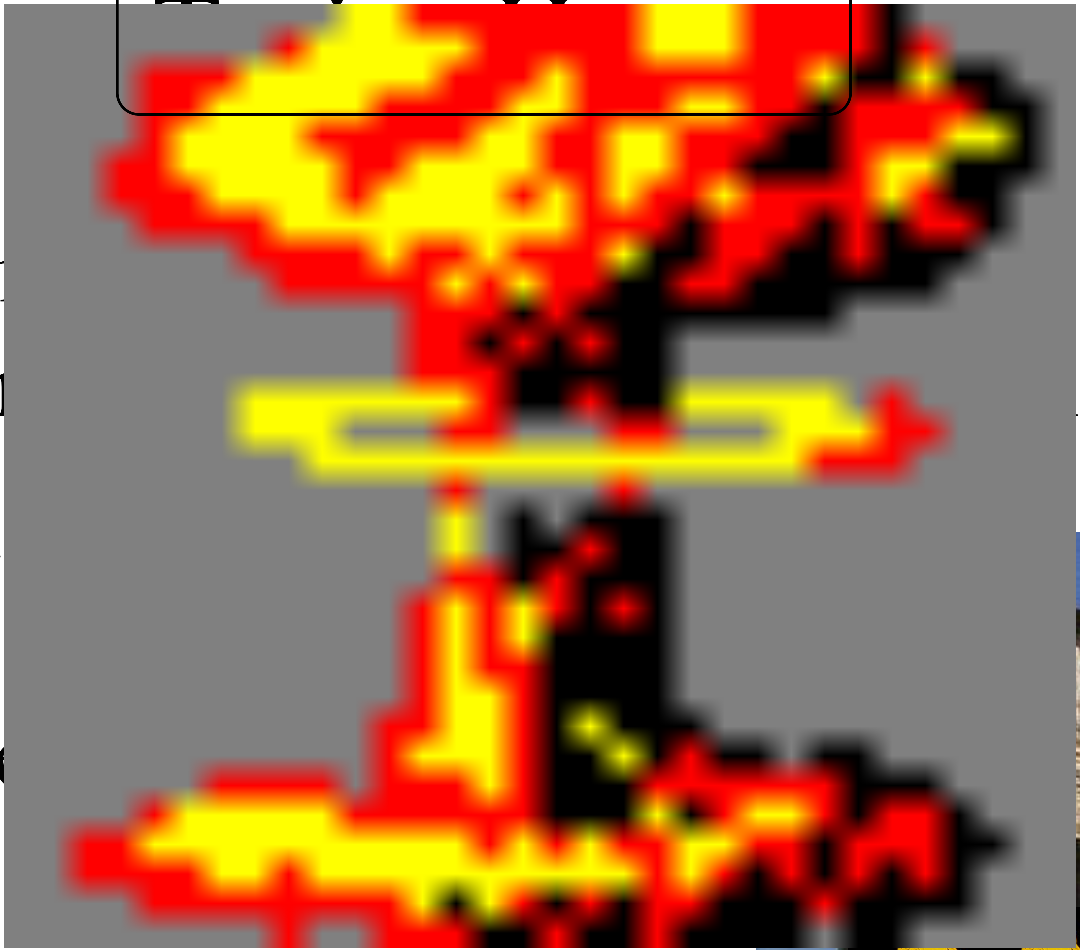
- Seemi
  contai ings

- When
  Greeks
  slaught



Basic Trojan Horses

- A program you pick up somewhere that is supposed to do something useful
- And perhaps it does
  - But it also does something less benign
- Games are a common location host program
- Downloaded applets are also popular
- Frequently found in email attachments
- Bogus security products also popular
- Flash drives are a hardware vector

Recent Trends in Trojan Horses

- Hand of Thief Trojan specifically designed to attack Linux boxes
  - Which are often regarded as particularly safe . . .
- Trojan designed for Android being used in banking scams
- North Korea using Kimsuky Trojan to spy on South Korea
- Obad Trojan spreading via mobile machine botnets

Trapdoors

- Also known as back doors
- A secret entry point into an otherwise legitimate program
- Typically inserted by the writer of the program
- Most often found in login programs or programs that use the network
- But also found in system utilities

Trapdoors and Other Malware

- Malware that has taken over a machine often inserts a trapdoor
- To allow the attacker to get back in
  - If the normal entry point is closed
- Infected machine should be handled carefully to remove such trapdoors
  - Otherwise, attacker comes right back

Logic Bombs

- Like trapdoors, typically in a legitimate program
- Code that "explodes" under certain conditions
- Often inserted by program authors
- Previously used by primarily by disgruntled employees to get revenge
  - Former TSA employee got two years in prison for planting one in 2009
- Beginning to be a trick for nation state cyber attacks
  - South Korean banks and media companies hit with major logic bomb in March 2013

Extortionware

- Attacker breaks in and does something to system
  - Demands money to undo it
- Encrypting vital data is common
  - Some incidents also encrypted backups
- Unlike logic bombs, not timed or triggered

Worms

- Programs that seek to move from system to system
  - Making use of various vulnerabilities
- Other performs other malicious behavior
- The Internet worm used to be the most famous example
  - Blaster, Slammer, Witty are other worms
- Can spread very, very rapidly

The Internet Worm

- Created by a graduate student at Cornell in 1988
- Released (perhaps accidentally) on the Internet Nov. 2, 1988
- Spread rapidly throughout the network
  - 6000 machines infected

How Did the Internet Worm Work?

- The worm attacked vulnerabilities in Unix 4 BSD variants
- These vulnerabilities allowed improper execution of remote processes
- Which allowed the worm to get a foothold on a system
  - And then to spread

The Worm's Actions

- Find an uninfected system and infect that one
- Here's where it ran into trouble:
  - It re-infected already infected systems
  - Each infection was a new process
  - Caused systems to wedge
- Did not take intentional malicious actions against infected nodes

Stopping the Worm

- In essence, required rebooting all infected systems
  - And not bringing them back on the network until the worm was cleared out
  - Though some sites stayed connected
- Also, the flaws it exploited had to be patched
- Why didn't firewalls stop it?
  - They weren't invented yet

Effects of the Worm

- Around 6000 machines were infected and required substantial disinfecting activities
- Many, many more machines were brought down or pulled off the net
  - Due to uncertainty about scope and effects of the worm

What Did the Worm Teach Us?

- The existence of some particular vulnerabilities
- The costs of interconnection
- The dangers of being trusting
- Denial of service is easy
- Security of hosts is key
- Logging is important
- We obviously didn’t learn enough

Code Red

- A malicious worm that attacked Windows machines
- Basically used vulnerability in Microsoft IIS servers
- Became very widely spread and caused a lot of trouble

How Code Red Worked

- Attempted to connect to TCP port 80 (a web server port) on randomly chosen host
- If successful, sent HTTP GET request designed to cause a buffer overflow
- If successful, defaced all web pages requested from web server

More Code Red Actions

- Periodically, infected hosts tried to find other machines to compromise
- Triggered a DDoS attack on a fixed IP address at a particular time
- Actions repeated monthly
- Possible for Code Red to infect a machine multiple times simultaneously

Code Red Stupidity

- Bad method used to choose another random host
  - Same random number generator seed to create list of hosts to probe
- DDoS attack on a particular fixed IP address
  - Merely changing the target's IP address made the attack ineffective

Code Red II

- Used smarter random selection of targets
- Didn't try to reinfect infected machines
- Adds a Trojan Horse version of Internet Explorer to machine
  - Unless other patches in place, will reinfect machine after reboot on login
- Also, left a backdoor on some machines
- Doesn't deface web pages or launch DDoS
- Didn't turn on periodically

Impact of Code Red and Code Red II

- Code Red infected over 250,000 machines
- In combination, estimated infections of over 750,000 machines
- Code Red II is essentially dead
  - Except for periodic reintroductions of it
- But Code Red is still out there

Stuxnet

- Scary worm that popped up in 2010
- Targeted at SCADA systems
  - Particularly, Iranian nuclear enrichment facilities
- Altered industrial processes
- Very specifically targeted

Where Did Stuxnet Come From?

- Stuxnet was very sophisticated
  - Speculated to be from unfriendly nation state(s)
  - New York Times claims White House officials confirmed it (no official confirmation, though)
- Research suggests SCADA attacks do not need much sophistication, though
  - Non-expert NSS Labs researcher easily broke into Siemans systems
- Duqu worm might be Stuxnet descendent
  - Appears to be stealing certificates

Worm, Virus, or Trojan Horse?

- Terms often used interchangeably
- Trojan horse formally refers to a seemingly good program that contains evil code
  - Only run when user executes it
  - Effect isn't necessarily infection
- Viruses seek to infect other programs
- Worms seek to move from machine to machine
- Don't obsess about classifications