# Foundations of Computer Security

## Lecture 75: CodeRedII

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

# CodeRedII

On August 4, 2001, an entirely new worm began to exploit the buffer-overflow vulnerability in Microsoft's IIS webservers.

The code contains the string "CodeRedII" which became the name.

- When the worm infects a new host, it first determines if the system has already been infected.
- If not, the worm initiates its propagation mechanism, sets up a "backdoor" into the infected machine, becomes dormant for a day, and then reboots the machine.
- Begins a process of propogating itself (follows).

# CodeRedII Propogation

Launches 300 or 600 threads in propogation attempt.

CodeRedII generates a random IP address and then applies a mask to produce the addresses to probe.

- 1/8th of the time, probes a completely random IP address.
- 1/2 of the time, probes a machine in the same /8 (new IP address has same first 8 bits).
- 3/8ths of the time, probes a machine on the same /16 (same first 16 bits).
- Avoids probing addresses in 224.0.0.0/8 (multicast) and 127.0.0.0/8 (loopback).

Machines on the same network or subnet are likely to be running similar software.

# Danger of CodeRedII

Unlike CodeRed, CodeRedII neither defaces web pages on infected machines nor launches a Denial-of-Service attack.

Also unlike CodeRed, CodeRedII is not memory resident, so rebooting an infected machine does not eliminate CodeRedII.

Installs a mechanism for remote, root-level access to the infected machine. This backdoor allows any code to be executed, so the machines could be used as zombies for future attacks.

# Rates of Response

Studies showed that the rate of patching vulnerable machines varied widely. The attack began on July 19; on Aug. 14 the following statistics were estimated:

| **Country** | **Patched** | **Unpatched** |
|---|---|---|
| United Kingdom | 66% | 34% |
| United States | 60% | 40% |
| Canada | 58% | 42% |
| Germany | 56% | 44% |
| Netherlands | 46% | 54% |
| Japan | 39% | 61% |
| Australia | 37% | 63% |
| Korea | 20% | 80% |
| Taiwan | 15% | 85% |
| China | 13% | 87% |

A large number of machines remained vulnerable to the same or similar attack.

# Install Patches

[A report from Verizon Business] *covering 500 forensic investigations, involving 230 million compromised customer records, found that nine out of 10 breaches attributed to hacking attacks took advantage of a vulnerability for which a fix was available at least six months prior to the attack.*

# Lessons

- CodeRedII is a different worm, exploiting the same vulnerability as CodeRed.
- Uses a much more sophisticated propogation strategy.
- Users often don't patch machines, leaving a population of vulnerable hosts.

**Next lecture:** Certification