Foundations of Computer Security

Lecture 74: Anatomy of an Attack: CodeRed

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

DoS Case Study: CodeRed

On June 18, 2001 eEye publicized a buffer-overflow vulnerability in Microsoft's IIS webservers: inadequate bounds checking on some input buffers allows system-level execution of code.

On July 12, 2001, the CodeRed virus began attacking unpatched machines. It works as follows:

- If date is between 1st and 19th of the month, generate a random list of IP addresses and attempt to infect those machines.
- On 20th to 28th of the month, launch a DoS flooding attack on `www1.whitehouse.gov`.
- The worm also defaces some webpages with the words "Hacked by Chinese."

CodeRed

On July 13, 2001, investigators from eEye Digital Security worked overnight to analyze the worm. The called it "CodeRed" because of the CodeRed Mountain Dew they were drinking and because of the "Hacked by Chinese" message.

- The worm uses a *static seed* in its random number generator and thus generates identical lists of IP addresses on each infected machine.
- Each infected machine probed the same list of machines, so the worm spread slowly.
- The IP address for `www1.whitehouse.gov` was changed so the DoS attack failed.

CodeRed Analysis

- Because of flaws in the design, especially the static seed, CodeRed did very little damage.
- The CodeRed worm is memory resident. A machine can be disinfected by simply rebooting it.
- Once-rebooted, the machine remains vulnerable to repeat infection, likely since each newly infected machine probes the same list of IP addresses.

CodeRed Version 2

On July 19, 2001 a variant began to circulate that was identical but uses a *random seed* in the random number generator.

- This had a major impact: more than 359,000 machines were infected with CodeRed (version 2) in just fourteen hours.
- Version 2 had a much greater impact on global infrastructure due to the sheer volume of hosts infected and probes sent to infect new hosts.
- Wreaked havoc on some additional devices with web interfaces: routers, switches, DSL modems, and printers. They either crashed or rebooted when an infected machine attempted to send them a copy of the worm.

Lessons

- CodeRed is a classic computer worm, but contained several severe flaws.
- The CodeRed author quickly exploited a vulnerability and quickly adapted his code in the light of flaws.

Next lecture: CodeRedII