MIT OpenCourseWare
http://ocw.mit.edu

6.033 Computer System Engineering

Spring 2009

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.

**Preparation for Recitation 23**

Read the paper entitled *Exploiting Underlying Structure for Detailed Reconstruction of an Internet-Scale Event*. This paper describes how the authors analyzed the propagation tree of the Witty Worm and identified the host that started the attack. Read the abstract, and Sections 1, 2, 3, and 4.

Computer worms are self-propagating programs. A worm can be either benign or malicious. A malicious worm may try to destroy some files on the infected machine or use the machine to mount a denial of service attack on some Internet service, whereas a benign one uses the machine only to spread itself to other machines.

To infect a host, a worm exploits a security bug in the software running on that host. Once the worm infects a host, it uses that host to contact new destinations and propagate to new victims, thus creating a propagation tree. As a result worms propagate exponentially fast. One important characteristic of a worm is the method used for picking new destinations. The most common way is to randomly pick IP addresses and contact them to see whether they suffer from the same security bug exploited by the worm. If they are, then they become infected and they start propagating the worm to even more machines. Some worms do not pick destinations randomly; they rather have a hit list of IP addresses that suffer from the exploited bug. These worms can propagate faster because they focus on the vulnerable victims.

The paper uses a network telescope to passively collect information about the Witty worm. A network telescope is an unused chunk of the IP address space. A big telescope may be monitoring a /8 address prefix, while a small one may monitor a /24 prefix. Since IP addresses in the monitored space are not assigned to any Internet hosts, they theoretically should not receive any traffic. But because worms and other Internet attacks tend to send traffic to random IPs, in practice, an unused IP prefix receives a lot of attack traffic. The authors of the paper collected the Witty packets received at all IP addresses in the monitored space and analyzed it to understand how Witty propagated.

While reading about Witty, try to answer the following questions:

1. How does Witty pick the IP address of the next destination?
2. How did the authors identify patient zero (i.e., the machine that started the worm)
3. How could one change Witty to prevent the detection of patient zero?
4. Which factors affect how fast a worm propagates?