

Internet Worms

Haley Nguyen

March 7, 2008

Why we are studying worms

- This topic has a global scope.
- Internet worms are potentially an immense threat, and the threat has not gone away.
- Although worm threat has receded in the background because currently botnets are more efficient to generate attacks, it may be back because there is no definitive solution to the problem.
- Worms today are used to construct botnets.
- Much of the technology developed for worms also applies to botnets.
- Cyber-warfare will eventually happen.
- Since the arm race is a factor for the defense to keep up with the threat, the worry is that when the threat recedes, the defense slackens, so when the attack happens, the defense is not sufficient to protect the victims.

Definition of a worm A process that self-replicated across the network. This means it can execute without any help from the outside (user). Contagion worms execute without user help but require user activity.

How does it work

- find potential victim - targeting (typically by random scan)
- gain control - exploit (typically by buffer overflow)
- using control, instantiate copy (called the payload)

History of worms

- 1988, Morris (a topological, bi-platform worm / author), a grad student at Cornell. He wrote his worm, and it went after Vax Unix and SunOS operating systems. It exploited the VAX Unix by a buffer overflow. It exploited the SunOS by sendmail debug; this attack only utilizes the functionalities provided by the application.
- Once it get its hooks on a machine, it guesses password, mines local information (.rhosts, etc/hosts/equiv, .forward, routing table, scan beyond routing table). If the machine have a point to point link, it will try to find and attack it. This is a very powerful approach.
- The code is obfuscate, it deletes its binary, forks itself every few minutes and transfers control to the child, so the worm's PID keeps changing. All to resist forensics.
- The worm tries to detect infected machines to not infect them again.
- Most worms have significant bugs.
- You'll see estimates that it infected about 10% of the Internet at the time, but these don't appear to be based on any sound foundation.

Modern area - Code Red I

- Appeared first July 13th, 2001.
- Not nearly as innovative as Morris.
- Exploit a known flaw that was not fixed for over a month in IIS servers
- The worm injects code, pick random 32 bit number to locate victim, but every copy of the worm will have the same set of number
- Initial version of worm lacked seeding of random number generator, so every copy scanned the same set of addresses. This lead to linear rather than exponential growth.
- On July 19th, the worm was fixed for bugs, then it no longer defaced web server, and every copy no longer generated the same set of random IP address. It also targeted white house web server by IP address.
- On July 19th, 2001, as seen via measurements at LBL, the number of connection started rising between 7 AM and 10 AM, reached to maximum to 1800 new HTTP hosts (not seen previously that day) each minute. After it reached the maximum, then it started having trouble finding new victims.

- The worm propagated on the 19th, tried to flood White House server on the 20th. Since the worm was programmed to die if it failed to attack a server, and the White House web server was moved to a different IP address, the worm died on the 20th.
- There were a few infected machines on the Internet that used clocks that were off by many days, so the worm spread from those machine to others, switched phases and avoided death.
- Last seen at LBL on July 2003.

Code Red 2 Go after the same vulnerability as Code Red 1, but uses a different code base. Doesn't work on NT.

- It has localize scanning, prefers to scan address block near it.
- When it started, it was competitive with Code Red 1 and replaced Code Red 1 later.
- It installs a back door on infected machines.
- It is programmed to die.

Nimda

- Multi-mode like Morris
- Email itself like a virus
- It installs itself on open share: if you share an executable with someone else, it puts itself on the executable. (fly-by attack)
- It would access Code Red 2's back door to runs itself.
- Goes right through firewall.
- Institutions that didn't encounter Code Red 1 and 2 were completely unprepared to deal with Nimda. This is a demonstation that coexistence is healthy to develop defenses.
- Last seen at LBL 2008.

Slammer

- It spreads using UDP connections (the usual is TCP); its payload fits in a single packet
- Go after some Window database service.
- It can spread *very* fast by keeping sending itself off with one UDP sendto().

- It has a bandwidth-limited growth.
- The doubling constant for slammer is 8.5 seconds.
- At ICSI, last seen March 6th, 2008.

Blaster

- Appear on Aug 2003
- Goes after a ubiquitous Window service
- concurrent with a blackout in Northeast (just a distraction).
- Its payload was to attack Microsoft Window Update service.

Nachia / Welchia

- written to counteract Blaster, and install a back door

Witty *Note: the following was not presented in lecture. Witty will be covered in detail in the upcoming Forensics lecture.*

- First appeared on Mar 2004
- Attempts to overwrite 128 sectors on one of the first eight physical hard drives, selected at random. The worm selects a random location on the hard drive and overwrites it with data from memory. If the randomly selected physical hard disk does not exist, the worm will continue.
- Exploits ICQ parsing
- Sends itself to 20,000 randomly generated IP addresses with random destination ports and a UDP source port of 4000.

Samy

- Oct 2005
- A worm that exploits MySpace's cross-site scripting vulnerability.
- When users visit the worm's author page, user automatically sends a "friend invite." Once they become "friends," they have the text "but most of all, samy is my hero" in their self-description.
- No violation of semantics
- The worm's author was convicted but received no jail time.

Modeling Worm Spread

- Classic SI model
 1. N: vulnerable population size
 2. S(t): susceptible hosts at time t
 3. a(t): proportion of infected host at time t
 4. K: individual contact rate
 5. $Nda = (Na)K(1 - a)dt \Rightarrow \frac{da}{dt} = Ka(1 - a)$
 6. The models: as the infected population becomes saturated, the infection rate goes down.
- Infected victims have no reason to care as long as the infection does not tax them.
- Infected laptops can bring worms inside the network border.

Better worms

- Why there is a published paper on better worms: these methods are not hard to think up. Nick Weaver took a week to come up with these methods on his free time. Therefore, by publishing a paper we don't really give attackers anything they cannot have otherwise. Moreover, since this is a deep threat, we need to illustrate the threat to call for defense.
- The paper got a lot of people excited. It was posted in a mailing list of 20,000 people in it. Some of the replies were harshly critical in terms of framing the authors as wannabe "cyber-heroes."
- CDC has gotten nowhere.
- DARPA has funded more research on this, and eventually classified it to Top Secret.