

Security Topics in Networking and Distributed Systems CS 590D

Lecture 10: Worms (cont.)

Department of Computer Sciences
Purdue University

References

- Modeling the Spread of Active Worms. Zesheng Chen, Lixin Gao, Kevin Kwiat, INFOCOM 2003.
- Internet Quarantine: Requirements for Containing Self-Propagating Code. David Moore, Colleen Shannon, Geoffrey M. Voelker, Stefan Savage, INFOCOM 2003.
- How to Own the Internet in Your Spare Time, Stuart Staniford, Vern Paxson, Nicholas Weaver USENIX 2002



Worms



- Program that can replicate itself and send copies from computer to computer across network connections;
- Use network connections to spread from system to system.
- Within a system, can behave as a computer virus, or it could implant Trojan horse programs, or perform unwanted, disruptive or destructive functions.

Factors

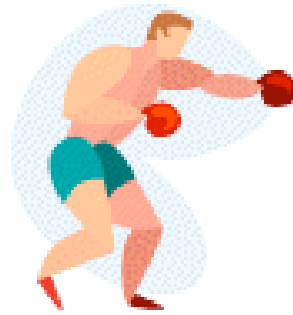
- **Target discovery**: mechanism by which a worm discovers new targets to infect.
- **Carrier**: mechanism the worm uses to transmit itself to the target.
- **Activation**: mechanism by which the worm's code begins operating on the target.
- **Payloads**: non-propagating routines a worm uses to accomplish a goal.
- **Attackers**: different goals.

Target Discovery

- **Scanning**: probing a set of addresses to identify vulnerable hosts:
 - **sequential**
 - **random.**
- **Using lists**
 - **Pre-generated target lists**: create a list of probable victims. **Externally generated target lists**: exploit the fact that some servers maintain lists of active servers, (games, peer-to-peer applications).
 - **Internal target list**: applications maintain information about servers with vulnerabilities; can be used to create topological worms
- **Passive**: wait for potential victim to contact the worm or rely on user behavior to discover new targets

Approach

- Prevention
- Detection
- Containment
- Response



Modeling Worm Propagation

- Why?
 - Can help detect worms
 - Prediction of spreading
 - Estimation of damage
- Factors?
 - Target discovery scanning, lists
 - Network topology
 - Network parameters: bandwidth, latency
 - Repair rate (applying patches)
 - Worm design specifics: transport protocol, amount of data transferred.



Models of Worm Propagation

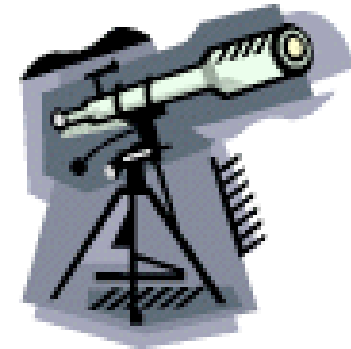
- Epidemiologic modeling
- Deterministic approximation modeling
- What did these models take into account?

Several Simulators

- Weaver simulator
- SSFnet
- EASEL
- DIB:S/TRAFEN

Other Ways of Detecting Worm Attacks

- Monitor for scanning.
- **When is the scanning perceived as being an attack?**
- Worms action results in denial of service, why not infer/estimate denial of service activity
- **How to infer/estimate denial of service activity?**



Network telescopes

Containment/Quarantine

- “Worm containment is the art, science, and engineering discipline of preventing worms from spreading”
 - <http://www.networm.org>
- Internet vs. enterprise containment
- Firewalls?
- Internal firewalls? Do they work? What are the limitations?
- Intrusion detection systems

Containment/Quarantine

- Containment of **scanning worms** (outbound vs. inbound scans)
- Containment of **flash worms** (develops a complete hitlist of all vulnerable systems, splits the list when infects a machine)
- Containment of **topological worms** (relies on information it finds on the infected host in order to locate further potential victims to infect)



If You Can Not Stop It, Slow It Down !!!

- LaBrea:, a "sticky honeypot"
 - Takes over unused IP addresses on a network and creates "virtual machines"
 - Answer to connection attempts in a way that causes the machine at the other end to get "stuck"
 - started in response to the CodeRed worm.

