



Internet Security: Surviving the Storm

Kathleen R. Kimball

Director, Security Operations and Services,
Information Technology Services

December 7, 2004

Storm Warnings

- Background: No computer is inherently secure; networks compound the issue
- Design, test and implementation decisions can help (or hurt), to include a fundamental choice between convenience and protection
 - Note: Reasonable protection can be convenient and largely transparent to users, but development costs accrue

Current State

- Bad by anyone's definition
- Constant probes (many successful)
- Security dependent to a large degree on the actions of non-technical users
 - Insecurity anywhere can affect the whole
- “Monoculture” can make the impact of a major attack more severe

By the Numbers

- 4,496
- 5.8
- 17

4,496

- The number of new Windows viruses and worms documented by Symantec from January to June 2004
 - More than four and a half times the number as the same period in 2003

5.8

- Average number of days between the public disclosure of a vulnerability and the release of an associated exploit that can be used to target it—often with the intent to take over computers remotely

17

- The survival time in minutes reported by the SANS Internet Storm Center for December 6th
- Survival time is defined as the average time between reported probes for an average network address/system
 - Assuming that most of these reports are generated by worms that attempt to propagate, a system that's not up-to-date with security patches would be infected by such a probe

Why? Converging Trends

- Sophistication level of the attacks is increasing
- Complexity of detecting and removing attack “residue” is similarly increasing – reformatting is often required
- The number of patches that must be applied is increasing as vendors respond to security concerns
- The time in which such patches must be universally applied is shrinking. Slow reaction time may lead to compromise
- Growth in mobility (Laptops and other mobile devices connecting to uncontrolled networks elsewhere and returning to infect the local environment)
- Growth of Internet-connected systems is increasing
 - Target Rich Environment

Effects of Trends

- Increasing mobility makes perimeter firewalls less useful—still needed but more is coming in behind them
- Patching, detection, prevention and remediation efforts need to match the sophistication level of the attacks
- Economic impetus (organized crime, identity theft, spamming et al). More sensitive data may be targeted
- Rising remediation costs
- Bots and rootkits are really problematic
 - Make scanning and some other traditional security methods that can be employed centrally less reliable

Digression: So What is a Bot Anyway?

- Bots –
 - Essentially a “robot”
 - People use robots to automate tedious tasks they don't want to do, and to do them more quickly and efficiently than a human could. In this case, bots automate network and system attacks
 - Combine many different forms of attack methods
 - Morph or change frequently – many bot variants
 - Implant different types of malicious software (to include programs to remotely control an infected computer and/or to capture keystrokes typed by user(s) on the keyboard)

Selected Bot Techniques (Cont.)

- Surreptitiously communicate back to whoever is controlling things
- “Rootkits” are often used to make detection difficult for even an experienced system administrator
 - Rootkits change system files to attempt to mask any trace of an intruder’s presence
- Bots become parts of “botnets” controlled by the same individual or group
 - May be sold – your machine has economic value
 - Both botnets and “phishing” schemes now being linked in some cases with organized crime
 - Some botnets are huge

Forecast

- Continued storm activity for several years to come
- What can be done?
 - University: perimeter network defenses, scanning, intrusion detection (and intrusion prevention where possible), education and awareness activities, national and regional influence
 - College/unit: same, plus automated patch management and anti-virus updates, potential for network access control, consider security in procurement decisions

Forecast (Continued)

- Individual Users
 - Personal firewalls
 - Current and updated anti-virus software
 - Current and updated operating system and application software
 - Anti-spyware software
 - Proper password selection and maintenance
 - Adequate backup and recovery strategies
 - Awareness and vigilance (avoid “phishing” and other social engineering attempts); avoid downloading freeware from suspicious sites

Forecast (Continued)

- Vendors
 - Ultimately where much of the solution must lie
 - Better, more security-conscious development practices
 - Security truly enabled by default on software intended for end user distribution
 - Limitation on what can be done at a system level by remote action
 - Detection and prevention higher in the overall network scheme
- Bottom line: Layered approach (Defense in Depth) rather than reliance on any one mechanism is essential. We're all in this together....

Questions???

As implied by a lot of what you saw today,
the answers are still evolving....

Presentation materials and background information are
available at: <http://sos.its.psu.edu/securitystate.html>