**Security**

- The Storm worm botnet is showing no signs of slowing down after three months in circulation. Estimates of the botnet’s size range from 2 million to 50 million infected computers worldwide. Security researchers are warning that the botnet could overpower the top supercomputers. Adam Swidler, a manager at Postini, says, “If you calculate pure theoretical throughput, then I’m sure the botnet has more capacity than BlueGene. If you sat them down to play chess, the botnet would win.” Accurate numbers on the botnet’s size and strength are unknown, but Matt Sergeant, MessageLabs’ chief anti-spam technologist, estimates that the botnet operates at roughly 10 percent of capacity on any given day.

- Security firm Panda Software’s quarterly report released in September details the malware industry’s efforts to provide one-stop shopping for its customers. Malware sites aren’t new, but crimeware writers are now expanding their efforts to include services such as encryption for their malware and spam server rentals. Competition between sites has even led to volume pricing for email lists and special offers, such as one site’s discount for the first 100 buyers of a Trojan. For more on this issue, please see Attack Trends on p. 69.

- In September, Symantec inadvertently issued an email notifying users of its DeepSight Threat Management System that the Internet was undergoing a full-scale attack. The alert raised the system’s ThreatCon level from one to four, which Symantec only uses when “extreme global network incident activity is in progress.” In a follow-up email, Symantec said the email was sent out in error as part of product testing. Symantec has never issued a level four alert, and level three alerts are just as rare. The last level three alert that Symantec issued was in 2004 at the height of the Sasser worm.

- Researchers at iDefense, a security firm based in Virginia, discovered a flaw that affects OpenOffice version 2.0.4 and earlier versions. The flaw could let attackers execute malicious code through TIFF files on Linux, Windows, and Mac computers. The flaw has been fixed in OpenOffice version 2.3.

- Google acknowledged a Gmail filtering vulnerability that could let attackers inject rogue filters into users’ filter lists that forward past and all future emails to their own inboxes. The attack — called a cross-site request forgery by the security researcher who discovered it — could start when users visit malicious Web sites while still logged into their Gmail accounts. The malicious site then launches an HTML command that injects an attacker-created filter into users’ accounts. Google has since fixed the vulnerability, but infected users’ email will continue to forward to the attacker’s email inbox until they remove the injected filter from their filter list.

- In October, Sun issued several patches to fix serious vulnerabilities in its Java Runtime Environment (JRE). The patches include a fix for a vulnerability that could let malicious Web sites bypass firewalls and security systems and access internal networks. Security firm Secunia strongly advised users of all Java platforms to apply the patches immediately.

- Security researchers have found several holes in the firewall for Apple’s Leopard operating system. Rich Mogull, founder of Securosis, says Leopard’s firewall lacks the flexibility that its predecessor, Tiger, has and must be manually configured. Jurgen Schmidt, a researcher from Heise Security, adds another cause for concern over the firewall is that it failed to block incoming connections after he had checked the “block all” setting.

**Privacy**

- US Senators Patrick Leahy (D-Vt.) and Arlen Specter (R-Pa.) introduced a bill that would let identity theft victims recover money and for the time spent repairing their credit histories. The bill would eliminate the requirement that victims’ suffer a minimum of US$5,000 in losses before they can prosecute. Additionally, the bill would also include digital extortion schemes in the definition of cybercrime. The bill is still before the Senate.

- America Online (AOL) announced its plan to offer consumers a Web site that links them to do-not-track lists run by the largest advertising networks, which will hide their Web browsing habits from advertisers. Users who use the lists will still see online ads, but advertisers won’t be able to push out ads tailored to them based on...
their Internet surfing. AOL expects to have the Web site up by the end of the year. The company made the announce-
ment at a privacy forum hosted by the US Federal Trade
Commission in October.

In October, Margaret Spellings, US Education Secre-
tary, issued privacy guidelines that aim to help edu-
cators and parents interpret what information can be shared under the 1974 Family Educational Rights and Privacy Act. The US Department of Education issued three brochures targeting K–12 educators, colleges, and parents. The guidelines are a response to the Virginia Tech shooting, in which a student killed 33 people. A panel ap-
pointed by Virginia Governor Timothy Kaine to investigate the shooting found confusion about the information that law enforcement and school officials could share with each other on the shooter.

A school district in Nashville, Tennessee, announced
plans to test face recognition technology in three of its
schools. In December, the school district will start install-
ing security cameras and taking digital photos of students and administrators. The school district plans to use the face recognition technology to spot intruders. However, Jonathon Phillips, leader of the face recognition program at the US National Institute of Standards and Technology, says the cameras have problems in poor lighting and with photographing faces at certain angles.

In November, the European Commission announced a
new proposal that would collect and send the personal
information—names, telephone numbers, credit-card in-
formation, travel itineraries, and so on—of passengers
flying into and out of Europe to EU states. Under the
proposal, the data would be kept for 13 years or longer if it’s used in criminal investigations or intelligence opera-
tions. The proposal doesn’t allow the collection of data
could reveal race, ethnicity, political opinions, reli-
gion, trade union membership, or health information.

Policy

The US Department of Homeland Security (DHS) has
ended the Analysis, Dissemination, Visualization, In-
sight and Semantic Enhancement (Advise) program, after spending US$42 million developing it. The DHS sus-
pended further development after its privacy office and
inspector general learned that testing of the program used real data from real people without meeting federal
privacy requirements.

A new bill before the US Senate Judiciary Committee
would extend retroactive immunity for companies
against lawsuits claiming illegal cooperation with gov-
ernment surveillance requests. The bill, sponsored by
John Rockefeller (D-W.Va.) and Christopher Bond (R-Mo.),
broadens the scope of existing law to include email provid-
ers, search engines, ISPs, and instant messaging services. Current law shields telecommunications companies who legally comply with government surveillance requests. The bill would shield companies such as Yahoo and Google from lawsuits and places the burden on the government to ensure that surveillance requests are legal.

In Austria, Maria Berger, Minister of Justice, and Gun-
ther Plater, Interior Minister, have proposed legislation
that would let Austrian police use Trojans to monitor
criminal suspects. The proposal limits the use of Trojans
to serious cases, such as terrorism and organized racketeer-
ing, and would require police to get a judge’s warrant be-
fore launching the Trojan. Critics of the proposal point out that specially designed Trojans could find their way into the malware community, causing even more problems. Geoff Sweeney, security researcher at Tier-3, says, “That scenario would create a serious free-for-all […] as legitimate Trojans are redirected to create an even more hostile environment for organizations to defend against.” Similar laws are being considered in Germany and Switzerland.

Anne Milgram, New Jersey’s Attorney General, has
asked four banks—Bank of America, Citibank, Washington Mutual, and Sun National Bank—to give her details on
how they respond to phishing attacks. The second part of
Milgram’s request asked that each bank advise its custom-
ers if it had been a recent phishing target—via email. Paul
Laudanski, leader of the Phishing Incident Reporting and Termination project, says, “The New Jersey Attorney Gen-
eral asking the banks to send out another email to clients is opening up […] those banks to being phished again.”

The Center for Strategic and International Studies
(CSIS) has created a cybersecurity commission filled with 32 cybersecurity experts. The commission’s goal is
to provide the next US president with a list of recom-
mandations that will help secure the government’s
networks. The commission’s co-chairs include Scott
Charney, Microsoft’s vice president for trustworthy com-
puting; Bobby Inman, former director of the US National
Security Agency; and US Representative Jim Langevin
(D-R.I.), chairman of the Homeland Security Subcom-
mittee on Emerging Threats, Cybersecurity and Science and Technology.