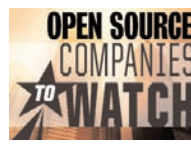




3G wireless not just for big shots anymore
EV-DO and other 3G mobile data services are taking hold across organizations such as Adidas. **Page 12.**



Newcomers exploit open source
Read about a new breed of companies targeting everything from Web search to virtualization to e-mail. **Page 16.**

NETWORKWORLD

Higher ed tackles convergence



Head of ACUTA trade group also has government regulations on his mind. **Page 14.**

TiVo records savings in compliance

Proactive stance, automation help firm save time and effort **Page 20.**

Vide Conferencing sidesteps telecommuters

Technology improvements and less-expensive bandwidth will help — eventually. **Page 34.**

Opinion: Vista vs. the Edsel

BackSpin Columnist Mark Gibbs compares the two. **Page 49.**



BackSpin Columnist Mark Gibbs compares the two. **Page 49.**

The leader in network knowledge ■ www.networkworld.com

August 27, 2007 ■ Volume 24, Number 33

HOW CLOSE IS WORLD WAR 3.0?



ED SCHNURR

Examining the reality of cyberwar in wake of Estonian attacks

BY CAROLYN DUFFY MARSAN

When the Estonian government was hit with major, sustained denial-of-service attacks this spring, the headlines screamed that it was the first incident of modern cyberwarfare.

The attacks disrupted a dozen government Web sites and networks run by ISPs, financial institutions and media outlets for several weeks in April and May. A global botnet of compromised home computers was used to create and direct the packet flood attacks that reached a peak of 90Mbps. Hackers also defaced key government Web sites with anti-Estonian slogans.

Pro-Russian activists were behind the cyberattacks, which were motivated by the Estonian government's decision to move a Soviet World War II memorial. The hackers launched hundreds of cyberattacks against Estonian Web sites, with attacks lasting less than one minute to 10 hours or more.

The Estonian attacks have left U.S. IT and network professionals wondering if they've entered a new era of cyberwar and what they should be doing to

See World War 3.0, page 22

HUAN TRAN

guide
TO ONLINE SECURITY

Risky e-business

Ten top industry veterans reveal their personal Web commerce habits and offer insider advice about how to conduct e-business safely. **Page 36**

NEWSPAPER ■ \$5.00



Avivah Litan

Tom Henderson

David Newman

Andreas Antonopoulos

World War 3.0

continued from page 1

prepare for politically motivated attacks.

Glen Baker, CIO of Outsource Partners Inc. (OPI), says he is "absolutely" concerned about the Estonia incident and the threat of politically motivated attacks against his company's network. The New York City firm does finance and accounting outsourcing for multinational companies, and it has the majority of its 1,500 employees in India and Bulgaria.

"We're in the process of hiring a security consulting firm to try to mitigate this threat," he says. "They will do analysis for us and build what a typical industry response should be."

Baker says OPI suffered Web defacements in 2001 and sees regular virus and spam attacks through incoming e-mail. He says he's more concerned about hacktivism than internal threats such as disgruntled employees.

"We have locked down facilities in India and Bulgaria. Users don't have many access rights or Internet access. They can't bring personal items on to our networks," Baker says. "But we do worry about external attacks. We can imagine political or anti-outsourcing attacks. Those are the ones we are trying to target and trying to mitigate."

Jose Nazario, senior security researcher with Arbor Networks, says CIOs in government and industry have been asking about the Estonian incident and whether it is evidence of a new online threat.

"As we move more critical infrastructure to the Internet and we depend on it more and more for communications, the threat [of cyberwar] is real," Nazario says. "It could be as specific as shutting down a phone system or it could be like the Estonian attacks, which



"If it really was a government-caused event, we would have seen something more damaging."

Charles Kaplan
Chief technology strategist at Mazu Networks

were hitting key government sites and mail servers. It could be both making a statement and disrupting an activity."

Security experts agree that despite the damage caused by the Estonian attacks, they were more hacktivism than all-out cyberwar. However, experts fear that we could be entering an era of more frequent politically motivated attacks and that commercial networks will be targeted.

Experts say the success of the Estonian attacks and the publicity they received may encourage other disgruntled individuals or groups to launch attacks. Companies with unpopular employment policies or business practices could be hit by similar attacks, they warn. "There is potential for [politically motivated attacks] to be more frequent based on the attention brought to what happened in Estonia," says Michael Witt, deputy director of the U.S. Computer Emergency Readiness Team within the Department of Homeland Security.

"We're sort of in uncharted territory," Witt adds. "You don't know what is going to upset an individual or a group to see if later they will launch a cyberattack."

Among the industries that could be targets for cyberattacks are not only ISPs and banks but also oil and electric companies.

"When you think about the citizens of many countries that may disappear beneath the ocean from global warming within 50 years, it's fairly easy to imagine a small, disaffected group [launching cyberattacks] because they're not being heard otherwise," says Eugene Spafford, executive director of the Center for Education and Research in Information Assurance and Security at Purdue University. "We have seen various groups because of racial or religious extreme ideologies ... circulating literature about bringing down utility grids."

Was it cyberwar?

Despite the initial headlines, most security experts say the Estonian incident wasn't cyberwarfare because it doesn't appear to have been sponsored by the Russian government.

"I would call it more of a political statement," Witt says.

Spafford says true cyberwarfare would be undertaken by one nation to bend another to its political will, and network attacks probably would be a companion to physical attacks.

"The activity that was carried out in Estonia was malicious and criminal," Spafford says. "If you look at some of the political demonstrations held in countries around the world, where traffic is brought to a standstill and there are work stoppages and banks are shut down as a matter of political statement, you wouldn't call that warfare."

Charles Kaplan, chief technology strategist at Mazu Networks, says the Estonian attacks appear to have been conducted by Russian citizens but weren't orchestrated by the Russian government.

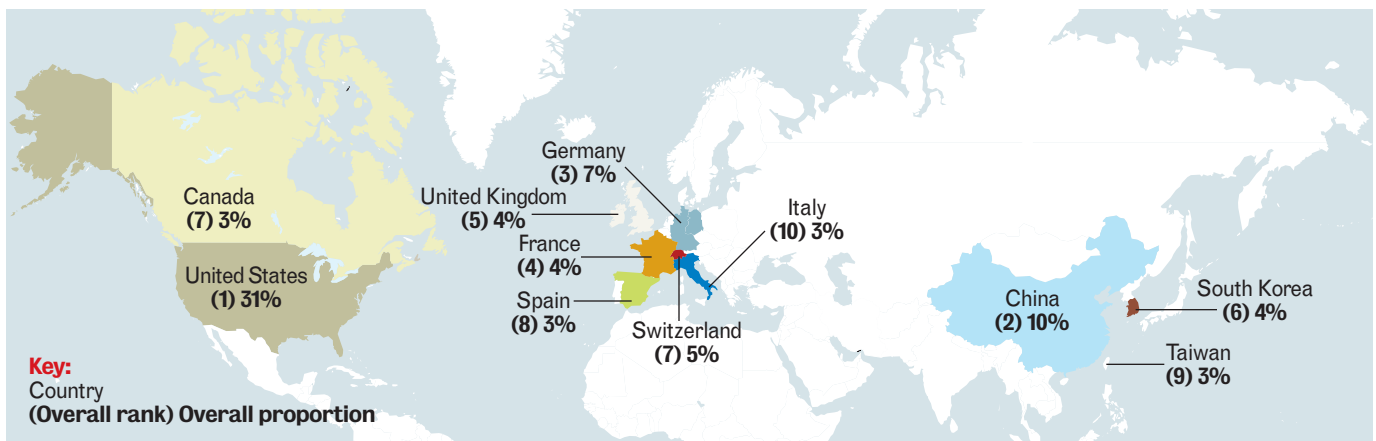
"If it really was a government-caused event, we would have seen something more damaging," Kaplan says. "This was a pure demonstration of brute force, and it did have some economic impact. If somebody really wanted to take these guys down, the damage would have been greater than it was."

See World War 3.0, page 24



Malicious activity by country

The overall ranking of the 10 worst countries for originating malicious Internet activity comes from individual rankings of the country's number of spam hosts, bot-infested computers, bot servers, phishing hosts, malicious code reports and Internet attacks. Although the few known incidents of cyberwarfare or significant hacktivism were from Russia and China, this shows that U.S. companies also need to worry about attacks from inside the United States given its big Internet infrastructure.



SOURCE: SYMANTEC REPORT ISSUED IN MARCH FOR PERIOD OF JULY 1 - DEC. 31, 2006

There are only two other known network attacks that were as devastating as the Estonian incident and have been called cyberwarfare. One, dubbed Titan Rain by the U.S. government, took place in 2003 and involved Chinese military attacks on networks run by Lockheed Martin, Sandia National Laboratories, Redstone Arsenal and NASA. The other incident, which the U.S. government refers to as Moonlight Maze, occurred in 1999 and involved Russian attacks on classified military information.

Whether it was cyberwar or hacktivism, the Estonian incident shows the devastation that a politically motivated network attack can have on government and commercial networks.

Security experts agree that it should be an eye-opener for CIOs, who have been focused on profit-oriented attacks and also should consider the threat of politically motivated ones.

Spafford calls the threat of political or ideological attacks against U.S. corporate networks significant. He points out that many early viruses and Web defacements were political statements.

"There are many organizations that may be targets for ideological groups because they do business somewhere in the world that may be unpopular," Spafford says. "If you're part of the banking or power industries, you may be a target for purposes of harm to the overall economy."

Spafford estimates that there are thousands of politically motivated attacks across the Internet each year. "Many of them aren't that coordinated or don't have as big of an impact as in Estonia," he says.

However, the majority of cyberattacks are economically motivated, with the most common targets being gambling, e-commerce, pornography and financial Web sites.

"We don't see a lot of denial-of-service attacks these days because most of the cyberattacks we see are profit motivated," says Steve Bellovin, an Internet security expert and professor of computer science at Columbia University. "The most common are extortion, especially against gambling sites."

Lessons learned from Estonia

The packet floods used in the Estonian DoS attacks were not new. What was unusual about these attacks was the duration and the disruption they caused, experts say.



"We don't see a lot of denial-of-service attacks these days because most of the cyberattacks we see are profit motivated."

Steve Bellovin
Internet security expert

10 steps to prepare for cyberwar

How IT execs can prepare for the worst

Security experts say CIOs should take the following steps to prepare for politically motivated network attacks:

1. Conduct a network inventory. You need to know what is on your network and what are the key network resources you must have available at all times to keep your business running. Make sure these resources are geographically and logically dispersed.

2. Keep your private network logically and physically separated from the public Internet. This way it can't be shut down by a denial-of-service attack. Have your network audited to ensure that you understand your dependence on the public Internet.

3. Be vigilant. You need to have an around-the-clock, seven-day-a-week operational team monitoring your networks. They need to have network cognizance. They need to know what your infrastructure is and be able to monitor it.

4. Educate your workforce about IT security practices. Train and educate your workforce. Employees need to be educated to know when something is not right, and they need to know whom to call to report it.

5. Have security policies and plans in place and test them regularly. Empower your information security officers and their teams to be able to defend your networks.

6. Know whom to call at your ISP in case of an emergency. Get in contact with your ISP's technical staff before you have a problem. Make sure your service-level agreement with your ISP is ade-

quate to protect your infrastructure.

7. Have a backup plan. CIOs need a disaster recovery plan in case their Internet connectivity is affected. The plan should take into consideration long-term outages.

8. Reduce your profile. Use physical defenses such as fences and security cameras, not just cyberdefenses. Don't publicize where your corporate headquarters are located.

9. Beware of insiders. The recent car bombings in London demonstrate that terrorists will infiltrate an organization and wait several years before launching an attack. That could occur in an IT department, too. Someone could insinuate himself into an organization over time or blackmail an employee.

10. Have an emergency response plan. If you don't have a response plan worked out and you fall under attack, you're going to have a problem. You should develop the plan in conjunction with your service providers. You should also know whom to contact in law enforcement.

Sources for this story: Jose Nazario (senior security researcher, Arbor Networks); Michael Witt (deputy director, U.S. CERT); Charles Kaplan (chief technology strategist, Mazu Networks); Eugene Spafford (executive director of the Center for Education and Research in Information Assurance and Security at Purdue University); Steve Bellovin, (professor of computer science, Columbia University)

tion they caused, experts say.

"The size and scale of these attacks in terms of the bandwidth and packets per second is in the middle in terms of what we have seen for these kinds of attacks," Nazario says. "But they lasted for weeks, not hours or days, which is much longer than we've seen for most of these attacks in the past. And the targets and the inferred motivation were geopolitical rather than economic or a simple grudge. That suggests we have turned a corner."

Spafford says what's important for U.S. companies to learn about the Estonian incident is

how much damage a small number of people with resources can do.

Another lesson learned from this incident is that the Estonian response — of admitting the problem and getting help from ISPs and international governments — was largely successful.

One suggestion for network managers is not to worry too much about figuring out where a cyberattack is coming from or why. Ed Amoroso, CSO at AT&T, says network managers should instead focus on mitigating the attack.

"For the day-to-day types of attacks people are dealing with, the goal of trying to determine where the attack originates remains very elusive because most of the attacks involve bots," Amoroso says. "It's so tempting in cybersecurity to say let's trace back the attack to see where it's coming from, and let's hypothesize what the geopolitical situation is. Let's assume if we see that it's an intense attack, that it's well funded. But it's just as likely to be a kid sitting in Brooklyn. That's one of the great difficulties of doing cybersecurity."

The good news for U.S. CIOs is that they are better positioned to defend themselves against similar DoS attacks because the United States is so much larger than Estonia and has a more robust network infrastructure.

“The country of Estonia is about the size of Rhode Island [based on population],” says Marty Lindner, a senior member of the technical staff at the U.S. Computer Emergency Readiness Team. “They only have so much infrastructure. When somebody decides to launch a DoS attack, all it takes is a little more energy than the size of your infrastructure to knock it over. The attacker here decided to take out 11 to 12 Web sites... If you take a big corporate network in the U.S., it is bigger and more robust than Estonia’s will ever be.”

Even though the U.S. network infrastructure is more robust than Estonia’s, hacktivism and other politically motivated attacks are still a worry for CIOs, Witt says.

“We have worked diligently with our critical infrastructure owners and operators, whether in the telecom industry or the IT industry or the chemical or energy sectors,” Witt says. “We’ve been working at this for many years to make sure we have a more robust type of backbone to deal with this kind of attack. Is that to say we are 100% protected against this type of attack? Absolutely not. It all comes back to best practices and having plans in place to deal with attacks.”

What will happen next?

Security experts predict that politically motivated attacks will be more targeted than all-out cyberwar aimed at taking down the Internet.

“What motive would Russia or China have to try to take out the U.S. suddenly? If they do that, they’re going to get hurt, too,” Bellovin says. “If they take out the internets, they take them out for themselves, too. If they take out our economy, they take out some of their big trading partners, which hurts them, too. There’s not an obvious motive for something happening on that scale in the very near future.”

Bellovin says the more likely scenario is that hacktivists or cyberterrorists would disrupt individual commercial or government targets.

“What if someone said: Pay us \$100 million or the denial-of-service attack that took out the electrical grid in California is going to happen again?” Bellovin asks. “That would be an act of war. And from a military perspective, every major country is looking at attacks and defenses on this issue.”

Kaplan says politically motivated attacks are more likely to come in the form of spear phishing attacks rather than DoS attacks like those used against Estonia.

“If I want to steal a piece of information from a particular company or government, I just look around at publicly available information such as Google, find the controller of that information and send that particular person a phishing e-mail,” Kaplan explains. “He’s the only one who gets it, and it’s specific enough that he opens it up. I can’t do that on a mass scale, but I can do it to get deep into a particular organization.”

Kaplan also worries about hard-to-detect polymorphic viruses and malware hiding in virtualization engines. “When I think about what a group of kids or terrorists could do, there are so many other options that are more attractive than all-out governmental cyberwarfare,” he says.

Experts say what will happen next in cyberwar is that hacktivists will launch whatever kinds of attacks — DoS, Web defacements, worms, viruses, phishing or pharming — that help them meet their goals.

“It’s an arms race,” Lindner says. “The best thing that a corporation or anyone can do is have a good layered defense, understand their exposures and have a good plan for managing the attacks when they occur.”

Most of the steps that CIOs should take to prepare for hacktivism involve keeping up with state-of-the-art security practices. And these steps will protect networks from both political and profit-driven attacks.

“You shouldn’t neglect politically motivated attacks as a threat, but you should be worrying much more about the economic impact today,” Bellovin says. “Most of the things you should do about that would help to protect you against this threat as well.” ■

ONLINE: MORE WORLD WAR 3.0 COVERAGE

- Q&A with Homeland Security’s Michael Witt on the rise of hacktivism.
- What Estonia did right in snuffing out denial-of-service attacks.
- Polls/discussion forum: Tell us how worried you are about a potential cyberwar involving the United States and whether your organization has ever fallen victim to hacktivism. www.nwdocfinder.com/1357