Editors: Michael Lesk, lesk@acm.org
Martin R. Stytz, mstytz@att.net
Roland L. Trope, roland.trope@verizon.net

The New Front Line

Estonia under Cyberassault

Michael Lesk
Rutgers University

During the night of 26 April 2007, the Estonian government moved the Bronze Soldier—a memorial statue honoring Soviet World War II war dead—from the central square of its capital city, Tallinn, to a cemetery on the city's outskirts. Russians in Estonia and Russia protested, as did various Russian parliament members, officials from former Soviet Union countries, and the Patriarch of Moscow, the Russian Orthodox Church's spiritual leader. Riots broke out in Tallinn, leaving one dead, several hundred injured, and more than a thousand arrested (http://news.bbc.co.uk/2/hi/europe/6602171.stm). The Russian parliament called for the Estonian government's resignation, and the state-owned Russian Railways announced it would cancel passenger trains running between St. Petersburg and Tallinn. Simultaneously, distributed denial-of-service (DDoS) attacks began against Estonian computers.

Have we seen the first national cyberwar?

Estonia, although small (half the size of the US state of Maine, with roughly 1.3 million residents), is a remarkably Web-dependent country, with widespread Internet access, digital identity cards, an 80-percent usage rate for online banking, electronic tax collection, and remote medical monitoring.[1,2] The BBC reported that Estonia was more technologically advanced than France or Italy when it joined the European Union (EU) in 2004.[1] In 2006, Estonia had a broadband subscriber penetration rate of 16.6 percent, compared with 19.7 percent in the US and 14 percent in Italy, according to the Economist Intelligence Unit (http://globaltechforum.eiu.com/index.asp?layout=rich_story&channelid=4&categoryid=29&title=Estonia%3A+Learning+by+example&doc_id=10766). According to the *Christian Science Monitor*, the Estonian Parliament declared Internet access a "fundamental human right" in 2000, and Mart Laar (Estonian Prime Minister from 1992–94 and 1999–2002) declared that Estonia was "the first paperless government."[2] Estonia is so proud of its high technology that it calls itself "E-stonia," and its citizens can vote over the Internet (http://news.bbc.co.uk/2/hi/technology/3673619.stm).

The DDoS attacks began on the foreign minister's Web site, but spread to all government institutions and key businesses, such as banks. Estonia accused Russia of orchestrating the attack; Estonian Minister of Justice Rein Lang claimed the attacks could be traced to IP addresses in Moscow owned by the Russian government.[3] The Russian government denied responsibility, and outside experts found the evidence of official government involvement weak. Mikko Hypponen, chief research officer at security company F-Secure, feels that the attacks would've been more effective if the Russian government *had* been involved.[3] Certainly, many informal postings on the Internet asked Russians to participate (www.mercurynews.com/search/ci_5941544).

Jose Nazario of Arbor Networks recently posted attack measurements (http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/). He found that most of the attacks were Internet Control Message Protocol (ICMP) floods (that is, lots of "pings"). The maximum bandwidth used was roughly 90 Mbps, with 10 attacks lasting 10 hours or more. Although the media portrayed this in apocalyptic terms—Mark Landler and John Markoff of the *International Herald Tribune* described it as "downloading the entire Windows XP operating system every six seconds for 10 hours"[4]—it isn't actually that much data. Plenty of corporations have that much bandwidth; in Japan, for example, it costs roughly US$50 per month to obtain 100 Mbps. Estonia's problem is that it's a very small country, and its systems aren't configured for that kind of load.

By comparison, in May 2006, the antispam company Blue Security was forced to shut down by a retaliating spammer who used tens of thousands of machines in a DDoS attack amounting to 2 to 10 Gbps of fake traffic (www.itaniumsolutionsalliance.org/news/whitepapers_brochures/Sercure64_Surviving_DNS_DDoS.pdf).

What does a botnet cost?

Botnet operators have gone com-

mercial. They sell their services to spammers, and buy and steal zombie networks from each other; for example, Jay Echouafni, CEO of Orbit Communication (a satellite TV retailer), is accused of paying three botnet owners to attack his competitors' Web sites using zombie networks of 3,000 to 10,000 computers.[5] Echouafni is now a fugitive, but one of the botnet operators admitted to causing the DDoS attacks in a plea bargain.[6]

So what's the price of a botnet? The Shadowserver Foundation, a volunteer malware watchdog group, estimates that botnets cost between US$5,000 and $7,500, but that prices are actually falling and could go as low as $0.25 per bot.[7] Professor Andrea Matwyshyn at the University of Florida suggests that 5 million zombie computers currently exist, and spammers can rent botnets for $.05 to 0.10 per minute.[8] MSNBC's Bob Sullivan quotes $5,000 per day for a botnet of 50,000 to 70,000 PCs in his description of the wars between botnet owners trying to steal each other's machines (http://redtape.msnbc.com/2007/04/virus_gang_warf.html). In the same article, Portland State professor Craig Schiller estimates the cost of the attack on Blue Security at $1 million, or $2,000 per hour—an attack 20 to 100 times larger than the Estonian attack.

Suppose you wanted to hire a botnet to generate 100 Mbps of traffic. You might think that 100 broadband customers would suffice, but that's an unreasonable assumption. First, zombie nodes are less likely to be on machines with broadband connections; in theory, users who care that much about their network connections probably also care about up-to-date security software. Second, if a computer is blasting out as many messages as it possibly can, the local ISP would notice it, and might well decide to quarantine it (assuming the local ISP is a responsible organization with ethical business practices). So perhaps 10,000 computers would be a better choice, but this would still be only a few thousand dollars. A reasonable estimate for each attack would be $2,000; thus, the several dozen attacks against Estonia might have cost in the neighborhood of $100,000.

What this means is that the size of the attack doesn't imply government involvement. The amount of money needed to launch the attacks is easily within the capacity of a group of middle-class terrorists, nationalistic fervor notwithstanding.

Cyberwars

In John Brunner's 1974 novel, *The Shockwave Rider*, multiple computer worms attack each other and attempt to destroy network services. The Xerox Palo Alto Research Center (PARC) group that designed the first computer worm in 1978 cited the novel as inspiration. Although it didn't use the word "cyberwar" (first seen in a Chicago newspaper in 1991, according to the *Oxford English Dictionary*), the novel had the idea.

Surely, previous nationalistic hacker attacks have occurred. Dorothy Denning, for example, describes incidents in 2000 when Israeli and Palestinian hacker groups attacked the Web sites of Hezbollah and the Israeli Foreign Ministry, respectively.[9] She also mentions that Tamil groups sent 800 emails a day to Sri Lankan embassies in 1998 (today, that's hardly worth noticing). Several other incidents involved China. In May 1999, a US missile destroyed the Chinese embassy in Belgrade, and Chinese hackers overwrote the US Beijing embassy's Web page with "Down with Barbarians." Then, in August 1999, China and Taiwan exchanged Web site attacks, apparently following a Chinese statement insulting the Taiwanese president. Perhaps the most publicized incident occurred in 2001 after a US reconnaissance airplane collided with a Chinese jet fighter. US and Chinese hackers exchanged Web attacks, defacing between 1,000 and 2,000 Web sites in the US and China.

All of these incidents, however, involved attempts to overwrite Web sites with embarrassing and childish messages; they don't seem to be

something that governments would waste their effort on. Most seemed to be the actions of uncoordinated agents, although one group that did identify itself was the Electronic Disturbance Theatre, which claimed to support social change, in particular the Zapatista rebels in Mexico. It created a tool called FloodNet, a Java applet that implements "virtual sit-ins" by continuously reloading a targeted Web site.[9]

Such political activities are now rare for botnets, though. Currently, their main focus is spam, with roughly 90 billion messages sent per day. The Nigerian 419 scam (asking people to lend their banking information to someone who claims to be looking for a way to deposit stolen money in a Western bank) is allegedly worth US$3 billion a year (www.ultrascan.nl/assets/applets/2006_Stats_on_419_AFF_jan_23_2007_1.pdf). From the standpoint of those defending against cyberwar, the problem is that the existence of lucrative spamming businesses keeps the botnets in operation and motivated to stick around and fight software security companies.

Can we stop this?

Estonia was, in the end, unable to effectively counter the attack. It cut its Internet connections to the outside world so that people within Estonia could continue to use their conventional services. This, for example, made it difficult for people with Estonian bank cards to use ATMs in other countries. The attacks slowed down after 10 May (in Russia, Victory in Europe Day [V-E Day] commemorates on 9 May). Whoever was paying for the botnets probably stopped.

We would like to think that as software improves, botnets will become more difficult to build. However, it doesn't appear that even those machines running Vista are immune from viruses. Worse yet, in several parts of the world, most people run pirated software; the pirated-software suppliers, of course, don't care whether the software they deliver has up-to-date security features. In fact, they'd probably rather supply software with holes so they can then sell access to those vulnerabilities to spammers. Thus, even if spam stops originating in the US as more computers acquire decent antivirus software and ISPs get better about quarantining infected systems, botnets in the rest of the world are likely to continue.

Even if spam stops originating in the US as more computers acquire decent antivirus software and ISPs get better about quarantining the infected systems, botnets are likely to continue.

What steps should we take? In fairness, cyberwar is a lot less frightening than real war. Nobody died as a result of the cyberattacks, whereas the riots in Tallinn did kill someone. Similarly, the DDoS attacks on *Jyllands-Posten's* Web site and other Danish sites during the controversy over cartoons depicting Mohammed[10] justifiably received far less attention than the burnings of three embassies and the deaths of at least 45 people (www.msnbc.msn.com/id/11383819/).

Nevertheless, the US National Cyber Security Division's 2007 budget is $93 million (www.whitehouse.gov/omb/budget/fy2007/dhs.html), compared to billions in spam losses just from lost productivity due to deleting bad emails and software security purchases (www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12). The US lost $70 million to bank robberies last year, but the US Federal Bureau of Investigation's (FBI's) budget for criminal investigations is more than $2 billion (www.usdoj.gov/jmd/2005summary/html/p112-120.htm). Private companies spend far more on computer security than the government, but we undoubtedly need greater resources for centralized computer security investigations. Cooperation with similar agencies in foreign governments is also essential.

But signs of a changing attitude are appearing on the landscape. On 14 June 2007, the FBI announced that "Operation Bot Roast" had identified and indicted several major botnet operators. This represents a high-visibility acknowledgment that closing down botnets is important to reduce fraud and avoid national security threats (http://news.moneycentral.msn.com/provider/providerarticle.aspx?feed=AP&Date=20070613&ID=7031622).

Additionally, more educational efforts to persuade users to install security software would be useful; in fairness, this would help individual computer owners much more than the general public. It isn't necessary to appeal to altruism to get users to install anti-zombie software because the viruses that take over their machines are likely to look through them for credit-card numbers as well. Again, the biggest difficulty is likely to be users of pirated software who aren't willing to buy anything, including security software.

ISPs can be expected to become more vigilant for problematic subscribers and be quicker to quarantine infected users. As individuals come to depend more on their home computers, this could produce problems: imagine users whose 911 emergency service depends on voice-over-IP (VoIP) but can't access the Internet because their ISPs have quarantined their infected machines.

This is no worse, of course, than people who can't call 911 because they haven't paid their phone bill.

On balance, the Estonian cyberwar ought to be a wake-up call. Producing so much disruption for so little money has to be attractive to many groups. We know that people with evil intentions watched what happened; we can only hope that people with good intentions watched as well. □

References

1. O. Lungescu, "Tiny Estonia Leads Internet Revolution," *BBC News*, 7 Apr. 2004; http://news.bbc.co.uk/2/hi/europe/3603943.stm.
2. C. Woodward, "Estonia, Where Being Wired is a Human Right," *Christian Science Monitor*, 1 July 2003; www.csonline.com/2003/0701/p07s01-woeu.html.
3. M. Rantanen, "Virtual Harassment, But For Real," *Helsingin Sanomat*, 6 May 2007; www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868.
4. M. Landler and J. Markoff, "In Estonia, What May Be the First War in Cyberspace," *Int'l Herald Tribune*, 28 May 2007; www.iht.com/articles/2007/05/28/business/cyberwar.php.
5. K. Poulsen, "FBI Busts Alleged DDoS Mafia," *Security Focus*, 28 Aug. 2004; www.securityfocus.com/news/9411.
6. K. Poulsen, "Hackers Admit to Wave of Attacks," *Wired News*, 8 Sept. 2005; www.wired.com/politics/security/news/2005/09/68800.
7. L. Zeltser, "So Long Script Kiddies," *Information Security Magazine*, May 2007; http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1257131,00.html.
8. A. Matwyshyn, "Penetrating the Zombie Collective: Spam as an International Security Issue," *SCRIPT-ed*, vol. 3, no. 4, 2006; www.law.ed.ac.uk/ahrc/script-ed/vol3-4/matwyshyn.asp.
9. D. Denning, "Cyberwarriors: Activists and Terrorists Turn to Cyberspace," *Harvard Int'l Rev.*, vol. 23, no. 2, 2001; http://hir.harvard.edu/articles/905/.
10. M. Malkin, "The Islamists' War on the Internet," 15 Feb. 2006; www.michellemalkin.com/archives/004535.htm.

***Michael Lesk** is a professor and chair of the library and information science department at Rutgers University. His research interests include digital libraries, computer networks, and databases. Lesk has a PhD in chemical physics from Harvard University. He is a member of the National Academy of Engineering, the ACM, the IEEE, and the American Society for Information Science and Technology (ASIS&T). Contact him at lesk@acm.org.*