Cyber Assaults on Estonia Typify a New Battle Tactic

By Peter Finn
Washington Post Foreign Service
Saturday, May 19, 2007; A01

TALLINN, Estonia, May 18 -- This small Baltic country, one of the most wired societies in Europe, has been subject in recent weeks to massive and coordinated cyber attacks on Web sites of the government, banks, telecommunications companies, Internet service providers and news organizations, according to Estonian and foreign officials here.

Computer security specialists here call it an unprecedented assault on the public and private electronic infrastructure of a state. They say it is originating in Russia, which is angry over Estonia's recent relocation of a Soviet war memorial. Russian officials deny any government involvement.

The NATO alliance and the European Union have rushed information technology specialists to Estonia to observe and assist during the attacks, which have disrupted government e-mail and led financial institutions to shut down online banking.

As societies become increasingly dependent on computer networks that cross national borders, security experts worry that in wartime, enemies will attempt to cripple those networks with electronic attacks. The Department of Homeland Security has warned that U.S. networks should be secured against al-Qaeda hackers. Estonia's experience provides a rare chance to observe how such assaults proceed.

"These attacks were massive, well targeted and well organized," Jaak Aaviksoo, Estonia's minister of defense, said in an interview. They can't be viewed, he said, "as the spontaneous response of public discontent worldwide with the actions of the Estonian authorities" concerning the memorial. "Rather, we have to speak of organized attacks on basic modern infrastructures."

The Estonian government stops short of accusing the Russian government of orchestrating the assaults, but alleges that authorities in Moscow have shown no interest in helping to end them or investigating evidence that Russian state employees have taken part. One Estonian citizen has been arrested, and officials here say they also have identified Russians involved in the attacks.

"They won't even pick up the phone," Rein Lang, Estonia's minister of justice, said in an interview.

Estonian officials said they traced some attackers to Internet protocol (IP) addresses that belong to the Russian presidential administration and other state agencies in Russia.

"There are strong indications of Russian state involvement," said Silver Meikar, a member of Parliament in the governing coalition who follows information technology issues in Estonia. "I can say that based on a
A wide range of conversations with people in the security agencies."

Russian officials deny that claim. In a recent interview, Kremlin spokesman Dmitri Peskov called it "out of the question." Reached Friday at a Russia-E.U. summit, he reiterated the denial, saying there was nothing to add.

A Russian official who the Estonians say took part in the attacks said in an interview Friday that the assertion was groundless. "We know about the allegations, of course, and we checked our IP addresses," said Andrei Sosov, who works at the agency that handles information technology for the Russian government. His IP address was identified by the Estonians as having participated, according to documents obtained by The Washington Post.

"Our names and contact numbers are open resources. I am just saying that professional hackers could easily have used our IP addresses to spoil relations between Estonia and Russia."

Estonia has a large number of potential targets. The economic success of the tiny former Soviet republic is built largely on its status as an "e-society," with paperless government and electronic voting. Many common transactions, including the signing of legal documents, can be done via the Internet.

The attacks began on April 27, a Friday, within hours of the war memorial's relocation. On Russian-language Internet forums, Estonian officials say, instructions were posted on how to disable government Web sites by overwhelming them with traffic, a tactic known as a denial of service attack.

The Web sites of the Estonian president, the prime minister, Parliament and government ministries were quickly swamped with traffic, shutting them down. Hackers defaced other sites, putting, for instance, a Hitler mustache on the picture of Prime Minister Andrus Ansip on his political party's Web site.

The assault continued through the weekend. "It was like an Internet riot," said Hillar Aarelaid, a lead specialist on Estonia's Computer Emergency Response Team, which headed the government's defense.

The Estonian government began blocking Internet traffic from Russia on April 30 by filtering out all Web addresses that ended in .ru.

By April 30, Aarelaid said, security experts noticed an increasing level of sophistication. Government Web sites and new targets, including media Web sites, came under attack from electronic cudgels known as botnets. Bots are computers that can be remotely commanded to participate in an attack. They can be business or home computers, and are known as zombie computers.

When bots were turned loose on Estonia, Aaviksoo said, roughly 1 million unwitting computers worldwide were employed. Officials said they traced bots to countries as dissimilar as the United States, China, Vietnam, Egypt and Peru.

By May 1, Estonian Internet service providers had come under sustained attack. System administrators were forced to disconnect all customers for 20 seconds to reboot their networks.

Newspapers in Estonia responded by closing access to their Web sites to everyone outside the country, as did the government. The sites of universities and nongovernmental organizations were overwhelmed. Parliament's e-mail service was shut for 12 hours because of the strain on servers.
Foreign governments began to take notice. NATO, the United States and the E.U. sent information technology experts. "It was a concerted, well-organized attack, and that's why Estonia has taken it so seriously and so have we," said Robert Pszczel, a NATO spokesman. Estonia is a new member of NATO and the E.U.

The FBI also provided assistance, according to Estonian officials. The bureau referred a reporter's calls to the U.S. Embassy in Estonia, which said there was no one available to discuss American assistance to the Baltic State.

On May 9, the day Russia celebrates victory in World War II, a new wave of attacks began at midnight Moscow time.

"It was the Big Bang," Aarelaid said. By his account, 4 million packets of data per second, every second for 24 hours, bombarded a host of targets that day.

"Everyone from 10-year-old boys to very experienced professionals was attacking," he said. "It was like a forest fire. It kept spreading."

By May 10, bots were probing for weaknesses in Estonian banks. They forced Estonia's largest bank to shut down online services for all customers for an hour and a half. Online banking remains closed to all customers outside the Baltic States and Scandinavia, according to Jaan Priisalu, head of the IT risk management group at Hansabank, a major Baltic bank.

"The nature of the latest attacks is very different," said Linnar Viik, a government IT consultant, "and it's no longer a bunch of zombie computers, but things you can't buy from the black market," he said. "This is something that will be very deeply analyzed, because it's a new level of risk. In the 21st century, the understanding of a state is no longer only its territory and its airspace, but it's also its electronic infrastructure.

"This is not some virtual world," Viik added. "This is part of our independence. And these attacks were an attempt to take one country back to the cave, back to the Stone Age."

Post a Comment

View all comments that have been posted about this article.

Your washingtonpost.com User ID, furd, will be displayed with your comment.

You must be logged in to leave a comment. Log in | Register

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will