The New York Times
nytimes.com

May 29, 2007

Digital Fears Emerge After Data Siege in Estonia

By MARK LANDLER and JOHN MARKOFF

TALLINN, Estonia, May 24 — When Estonian authorities began removing a bronze statue of a World War II-era Soviet soldier from a park in this bustling Baltic seaport last month, they expected violent street protests by Estonians of Russian descent.

They also knew from experience that “if there are fights on the street, there are going to be fights on the Internet,” said Hillar Aarelaid, the director of Estonia’s Computer Emergency Response Team. After all, for people here the Internet is almost as vital as running water; it is used routinely to vote, file their taxes, and, with their cellphones, to shop or pay for parking.

What followed was what some here describe as the first war in cyberspace, a monthlong campaign that has forced Estonian authorities to defend their pint-size Baltic nation from a data flood that they say was set off by orders from Russia or ethnic Russian sources in retaliation for the removal of the statue.

The Estonians assert that an Internet address involved in the attacks belonged to an official who works in the administration of Russia’s president, Vladimir V. Putin.

The Russian government has denied any involvement in the attacks, which came close to shutting down the country’s digital infrastructure, clogging the Web sites of the president, the prime minister, Parliament and other government agencies, staggering Estonia’s biggest bank and overwhelming the sites of several daily newspapers.

“It turned out to be a national security situation,” Estonia’s defense minister, Jaak Aaviksoo, said in an interview. “It can effectively be compared to when your ports are shut to the sea.”

Computer security experts from NATO, the European Union, the United States and Israel have since converged on Tallinn to offer help and to learn what they can about cyberwar in the digital age.

“This may well turn out to be a watershed in terms of widespread awareness of the vulnerability of modern society,” said Linton Wells II, the principal deputy assistant secretary of defense for networks and information integration at the Pentagon. “It has gotten the attention of a lot of people.”

The authorities anticipated there would be a backlash to the removal of the statue, which had become a rallying point for Estonia’s large Russian-speaking minority, particularly as it was removed to a less accessible military graveyard.

When the first digital intruders slipped into Estonian cyberspace at 10 p.m. on April 26, Mr. Aarelaid figured he was ready. He had erected firewalls around government Web sites, set up extra computer servers and put his staff on call for a busy week.

By April 29, Tallinn’s streets were calm again after two nights of riots caused by the statue’s removal, but Estonia’s electronic Maginot Line was crumbling. In one of the first strikes, a flood of junk messages was thrown at the e-mail server of the Parliament, shutting it down. In another, hackers broke into the Web site of the Reform Party, posting a fake letter of apology from the prime minister, Andrus Ansip, for ordering the removal of the highly symbolic statue.

At that point, Mr. Aarelaid, a former police officer, gathered security experts from Estonia’s Internet service providers, banks, government agencies and the police. He also drew on contacts in Finland, Germany, Slovenia and other countries to help him track down and block suspicious Internet addresses and halt traffic from computers as far away as Peru and China.

The bulk of the cyberassaults used a technique known as a distributed denial-of-service attack. By bombarding the country’s Web sites with data, attackers can clog not only the country’s servers, but also its routers and switches, the specialized devices that direct traffic on the network.

To magnify the assault, the hackers infiltrated computers around the world with software known as bots, and banded them together in networks to perform these incursions. The computers become unwitting foot soldiers, or “zombies,” in a cyberattack.

In one case, the attackers sent a single huge burst of data to measure the capacity of the network. Then, hours later, data from multiple sources flowed into the system, rapidly reaching the upper limit of the routers and switches.

By the end of the first week, the Estonians, with the help of authorities in other countries, had become reasonably adept at filtering out malicious data. Still, Mr. Aarelaid knew the worst was yet to come. May 9 was Victory Day, the Russian holiday that marks the Soviet Union’s defeat of Nazi Germany and honors fallen Red Army soldiers. The Internet was rife with plans to mark the occasion by taking down Estonia’s network.

Mr. Aarelaid huddled with security chiefs at the banks, urging them to keep their services running. He was also under orders to protect an important government briefing site. Other sites, like that of the Estonian president, were sacrificed as low priorities.

The attackers used a giant network of bots — perhaps as many as one million computers in places as far away as the United States and Vietnam — to amplify the impact of their assault. In a sign of their financial resources, there is evidence that they rented time on other so-called botnets.

“When you combine very, very large packets of information with thousands of machines, you’ve got the recipe for very damaging denial-of-service attacks,” said Jose Nazario, an expert on bots at Arbor Networks, an Internet security firm in Ann Arbor, Mich.

In the early hours of May 9, traffic spiked to thousands of times the normal flow. May 10 was heavier still, forcing Estonia’s biggest bank to shut down its online service for more than an hour. Even now, the bank, Hansabank, is under assault and continues to block access to 300 suspect Internet addresses. It has had losses of at least $1 million.

Finally, on the afternoon of May 10, the attackers’ time on the rented servers expired, and the botnet attacks fell off abruptly.

All told, Arbor Networks measured dozens of attacks. The 10 largest assaults blasted streams of 90 megabits of data a second at Estonia’s networks, lasting up to 10 hours each. That is a data load equivalent to downloading the entire Windows XP operating system every six seconds for 10 hours.

“Hillar and his guys are good,” said Bill Woodcock, an American Internet security expert who was also on hand to observe the response. “There aren’t a lot of other countries that could combat that on his level of calm professionalism.”

Estonia’s defense was not flawless. To block hostile data, it had to close off large parts of its network to people outside the country.

“It is really a shame that an Estonian businessman traveling abroad does not have access to his bank account,” said Linnar Viik, a computer science professor and leader in Estonia’s high-tech industry. “For members of the Estonian Parliament, it meant four days without e-mail.”

Still, Mr. Viik said the episode would serve as a learning experience. The use of botnets, for example, illustrates how a cyberattack on a single country can ensnare many other countries.

In recent years, cyberattacks have been associated with Middle East and Serbian-Croatian conflicts. But computer systems at the Pentagon, NASA, universities and research labs have been compromised in the past.

Scientists and researchers convened by the National Academy of Sciences this year heard testimony from military strategy experts indicating that both China and Russia have offensive information-warfare programs. The United States is also said to have begun a cyberwarfare effort.

Though Estonia cannot be sure of the attackers’ identities, their plans were posted on the Internet even before the attack began. On Russian-language forums and chat groups, the investigators found detailed instructions on how to send disruptive messages, and which Estonian Web sites to use as targets.

“We were watching them being set up in real time,” said Mr. Aarelaid, who weeks later could find several examples using Google.

For NATO, the attack may lead to a discussion of whether it needs to modify its commitment to collective defense, enshrined in Article V of the North Atlantic Treaty. Mr. Aarelaid said NATO’s Internet security experts said little but took copious notes during their visit.

Because of the murkiness of the Internet — where attackers can mask their identities by using the Internet addresses of others, or remotely program distant computers to send data without their owners even knowing it — several experts said that the attackers would probably never be caught. American government officials said that the nature of the attacks suggested they were initiated by “hacktivists,” technical experts who act independently from governments.

“At the present time, we are not able to prove direct state links,” Mr. Aaviksoo, Estonia’s defense minister, said. “All we can say is that a server in our president’s office got a query from an I.P. address in the Russian administration,” he added, using the abbreviation for Internet protocol. Moscow had offered no help in tracking down people who the Estonian government believes may be involved.

A spokesman for the Kremlin, Dmitri S. Peskov, denied Russian state involvement in the attacks and added, “The Estonia side has to be extremely careful when making accusations.”

The police here arrested and then released a 19-year-old Estonian man of Russian descent whom they suspected of helping to organize the attacks. Meanwhile, Estonia’s foreign ministry has circulated a document that lists several Internet addresses inside the Russian government that it said took part in the attacks.

“I don’t think it was Russia, but who can tell?” said Gadi Evron, a computer security expert from Israel who spent four days in Tallinn writing a post-mortem on the response for the Estonians. “The Internet is perfect for plausible deniability.”

Mr. Evron, an executive at an Internet security firm called Beyond Security, is a veteran of this kind of warfare. He set up the Computer Emergency Response Team, or CERT, in Israel. Web sites in Israel are regularly subjected to attacks by Palestinians or others sympathetic to their cause.

“Whenever there is political tension, there is a cyber aftermath,” Mr. Evron said, noting that sites in Denmark became targets after a newspaper there published satirical cartoons depicting the prophet Muhammad.

The attacks on Estonia’s systems are not over, but they have dropped in volume and intensity, and are aimed mainly at banks. The last major wave of attacks was on May 18.

Now that the onslaught has ebbed, Mr. Aarelaid is mopping up. A few days ago, he managed to get to the sauna with Jaan Priisalu, the head of computer security at Hansabank, and other friends from Estonia’s Internet security fraternity.

“I’m a simple I.T. guy,” he said, gazing at a flickering computer screen. “I know a lot about bits and packets of data; I don’t know about the bigger questions. But somebody orchestrated this thing.”

Mark Landler reported from Tallinn and John Markoff from San Francisco. Steven Lee Myers contributed reporting from Moscow.

Privacy Policy | Search | Corrections | RSS | First Look | Help | Contact Us | Work for Us | Site Map