Vast Spy System Loots Computers in 103 Countries

By JOHN MARKOFF
Published: March 28, 2009

TORONTO — A vast electronic spying operation has infiltrated computers and has stolen documents from hundreds of government and private offices around the world, including those of the Dalai Lama, Canadian researchers have concluded.

Tim Leyes for The New York Times

The Toronto academic researchers who are reporting on the spying operation dubbed GhostNet include, from left, Ronald J. Deibert, Greg Walton, Nart Villeneuve and Rafal A. Rohozinski.

Multimedia

In a report to be issued this weekend, the researchers said that the system was being controlled from computers based almost exclusively in China, but that they could not say conclusively that the Chinese government was involved.

The researchers, who are based at the Munk Center for International Studies at the University of Toronto, had been asked by the office of the Dalai Lama, the exiled Tibetan leader whom China regularly denounces, to examine its computers for signs of malicious software, or malware.

Their sleuthing opened a window into a broader operation that, in less than two years, has infiltrated at least 1,295 computers in 103 countries, including many belonging to embassies, foreign ministries and other government offices, as well as the Dalai Lama's Tibetan exile centers in India, Brussels, London and New York.

The researchers, who have a record of detecting computer espionage, said they believed that in addition to the spying on the Dalai Lama, the system, which they called GhostNet, was focused on the governments of South Asian and Southeast Asian countries.

Intelligence analysts say many governments, including those of China, Russia and the United States, and other parties use sophisticated computer programs to covertly gather information.

The newly reported spying operation is by far the largest to come to light in terms of countries affected.

This is also believed to be the first time researchers have been able to expose the workings of a computer system used in an intrusion of this magnitude.

Still going strong, the operation continues to invade and monitor more than a dozen new computers a week, the researchers said in their report, “Tracking ‘GhostNet’: Investigating a Cyber Espionage Network.” They said they had found no evidence that United States government offices had been infiltrated, although a NATO computer was monitored by the spies for half a day and computers of the Indian Embassy in Washington were infiltrated.

The malware is remarkable both for its sweep — in computer jargon, it has not been merely “phishing” for random consumers’ information, but “whaling” for particular important targets — and for its Big Brother-style capacities. It can, for example, turn on the camera and audio-recording functions of an infected computer, enabling monitors to see and hear what goes on in a room. The investigators say they do not know if this facet has been employed.

The researchers were able to monitor the commands given to infected computers and to see the names of documents retrieved by the spies, but in most cases the contents of the stolen files have not been determined. Working with the Tibetans, however, the researchers found that specific correspondence had been stolen and that the intruders had gained control of the electronic mail server computers of the Dalai Lama’s organization.

The electronic spy game has had at least some real-world impact, they said. For example, they said, after an e-mail invitation was sent by the Dalai Lama's office to a foreign diplomat, the Chinese government made a call to the diplomat discouraging a visit. And a woman working for a group making Internet contacts between Tibetan exiles and Chinese citizens was stopped by Chinese intelligence officers on her way back to Tibet, shown transcripts of her online conversations and warned to stop her political activities.

The Toronto researchers said they had notified international law enforcement agencies of the spying operation, which in their view exposed basic shortcomings in the legal structure of cyberspace. The F.B.I. declined to comment on the operation.

Although the Canadian researchers said that most of the computers behind the spying were in China, they cautioned against concluding that China's government was involved. The spying could be a nonstate, for-profit operation, for example, or one run by private citizens in China known as "patriotic hackers."

"We're a bit more careful about it, knowing the nuance of what happens in the subterranean realms," said Ronald J. Deibert, a member of the research group and an associate professor of political science at Munk. "This could well be the C.I.A. or the Russians. It's a murky realm that we're lifting the lid on."

A spokesman for the Chinese Consulate in New York dismissed the idea that China was involved. "These are old stories and they are nonsense," the spokesman, Wenqi Gao, said. "The Chinese government is opposed to and strictly forbids any cybercrime."

The Toronto researchers, who allowed a reporter for The New York Times to review the spies' digital tracks, are publishing their findings in Information Warfare Monitor, an online publication associated with the Munk Center.

At the same time, two computer researchers at Cambridge University in Britain who worked on the part of the investigation related to the Tibetans, are releasing an independent report. They do fault China, and they warned that other hackers could adopt the tactics used in the malware operation.

“What Chinese spooks did in 2008, Russian crooks will do in 2010 and even low-budget criminals from less developed countries will follow in due course,” the Cambridge researchers, Shishir Nagaraja and Ross Anderson, wrote in their report, “The Snooping Dragon: Social Malware Surveillance of the Tibetan Movement.”

In any case, it was suspicions of Chinese interference that led to the discovery of the spy operation. Last summer, the office of the Dalai Lama invited two specialists to India to audit computers used by the Dalai Lama’s organization. The specialists, Greg Walton, the editor of Information Warfare Monitor, and Mr. Nagaraja, a network security expert, found that the computers had indeed been infected and that intruders had stolen files from personal computers serving several Tibetan exile groups.

Back in Toronto, Mr. Walton shared data with colleagues at the Munk Center’s computer lab.

One of them was Nart Villeneuve, 34, a graduate student and self-taught “white hat” hacker with dazzling technical skills. Last year, Mr. Villeneuve linked the Chinese version of the Skype communications service to a Chinese government operation that was systematically eavesdropping on users’ instant-messaging sessions.

Early this month, Mr. Villeneuve noticed an odd string of 22 characters embedded in files created by the malicious software and searched for it with Google. It led him to a group of computers on Hainan Island, off China, and to a Web site that would prove to be critically important.

In a puzzling security lapse, the Web page that Mr. Villeneuve found was not protected by a password, while much of the rest of the system uses encryption.

Mr. Villeneuve and his colleagues figured out how the operation worked by commanding it to infect a system in their computer lab in Toronto. On March 12, the spies took their own bait. Mr. Villeneuve watched a brief series of commands flicker on his computer screen as someone — presumably in China — rummaged through the files. Finding nothing of interest, the intruder soon disappeared.

Through trial and error, the researchers learned to use the system's Chinese-language "dashboard" — a control panel reachable with a standard Web browser — by which one could manipulate the more than 1,200 computers worldwide that had by then been infected.

Infection happens two ways. In one method, a user's clicking on a document attached to an e-mail message lets the system covertly install software deep in the target operating system. Alternatively, a user clicks on a Web link in an e-mail message and is taken directly to a "poisoned" Web site.

The researchers said they avoided breaking any laws during three weeks of monitoring and extensively experimenting with the system's unprotected software control panel. They provided, among other information, a log of compromised computers dating to May 22, 2007.

They found that three of the four control servers were in different provinces in China — Hainan, Guangdong and Sichuan — while the fourth was discovered to be at a Web-hosting company based in Southern California.

Beyond that, said Rafal A. Rohozinski, one of the investigators, "attribution is difficult because there is no agreed upon international legal framework for being able to pursue investigations down to their logical conclusion, which is highly local."