Researchers: Cyber spies break into govt computers

March 29 2009, By CHARMAINE NORONHA , Associated Press Writer

In this Tuesday March 10, 2009, file photo, Tibetan spiritual leader, the Dalai Lama, speaks to the media on the 50th anniversary of the Tibetan uprising against Chinese rule that sent him into exile, in Dharmsala, India. The South African government said Tuesday, March 24, 2009, that the Dalai Lama is not welcome until after the 2010 football World Cup, for fear tensions over Tibet would overshadow all other issues. Organizers said earlier that a peace conference scheduled in Johannesburg on Friday has been indefinitely postponed because the government had barred attendance by the Tibetan leader, who has clashed with China. Tibet's government-in-exile said South Africa was acting under pressure from China, but South Africa's government denied it. South Africa is China's largest African trading partner. (AP Photo/Ashwini Bhatia/file)

(AP) -- A cyber spy network based mainly in China hacked into classified documents from government and private organizations in 103 countries, including the computers of the Dalai Lama and Tibetan exiles, Canadian researchers said Saturday.

The work of the Information Warfare Monitor initially focused on allegations of Chinese cyber espionage against the Tibetan community in exile, and eventually led to a much wider network of compromised machines, the Internet-based research group said.

"We uncovered real-time evidence of malware that had penetrated Tibetan computer systems, extracting sensitive documents from the private office of the Dalai Lama," investigator Greg Walton said.

The research group said that while it's analysis points to China as the main source of the network, it has not conclusively been able to detect the identity or motivation of the hackers.

Calls to China's Foreign Ministry and Industry and Information Ministry rang unanswered Sunday. The Chinese Embassy in Toronto did not immediately return calls for comment Saturday.

Students For a Free Tibet activist Bhutila Karpoche said her organization's computers have been hacked into numerous times over the past four or five years, and particularly in the past year. She said she often gets e-mails that contain viruses that crash the group's computers.

The IWM is composed of researchers from Ottawa-based think tank SecDev Group and the University of Toronto's Munk Centre for International Studies. The group's initial findings led to a 10-month investigation summarized in the report to be released online Sunday.

The researchers detected a cyber espionage network involving over

1,295 compromised computers from the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan. They also discovered hacked systems in the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan.

Once the hackers infiltrated the systems, they gained control using malware - software they install on the compromised computers - and sent and received data from them, the researchers said.

Two researchers at Cambridge University in Britain who worked on the part of the investigation related to the Tibetans are also releasing their own report Sunday.

In an online abstract for "The Snooping Dragon: Social Malware Surveillance of the Tibetan Movement," Shishir Nagaraja and Ross Anderson write that while malware attacks are not new, these attacks should be noted for their ability to collect "actionable intelligence for use by the police and security services of a repressive state, with potentially fatal consequences for those exposed."

They say prevention against such attacks will be difficult since traditional defense against social malware in government agencies involves expensive and intrusive measures that range from mandatory access controls to tedious operational security procedures.

The Dalai Lama fled over the Himalaya mountains into exile 50 years ago when China quashed an uprising in Tibet, placing it under its direct rule for the first time. The spiritual leader and the Tibetan government in exile are based in Dharmsala, India.