E-mail messages to mailing lists and online forums are socially designed to infect computers with keylogger malware, security researchers said.

By Thomas Claburn, InformationWeek
March 21, 2008
URL:
http://www.informationweek.com/story/showArticle.jhtml?articleID=206905235

The attacks on mailing lists and online forums contain information related to recent events in Tibet and may appear to come from a trusted person or organization.

A shadow war against organizations supporting Tibetan protesters has erupted in cyberspace, mirroring efforts by Chinese authorities to quell unrest in the Tibet.

"Somebody is trying to use pro-Tibet themed e-mails to infect computers of the members of pro-Tibet groups to spy on their actions," said Mikko H. Hypponen, chief research officer at F-Secure, in a blog post on Friday. "And this is not an isolated incident. Far from it."

The cyberattack involves sending e-mail messages to mailing lists, online forums, and people known to be affiliated with pro-Tibet groups. To enhance their legitimacy, the messages contain information related to recent events in Tibet and may appear to come from a trusted person or organization.

But the content is simply bait, a social engineering con, to get recipients to open the documents and trigger an exploit. "The exploit silently drops and runs a file called C:\Program Files\Update\winkey.exe," explains Hypponen. "This is a keylogger that collects and sends everything typed on the affected machine to a server running at xsz.8800.org. And 8800.org is a Chinese DNS-bouncer system that, while not rogue by itself, has been used over and over again in various targeted attacks."

Efforts by Chinese authorities to contain protests in Tibet and limit media access to the country have been widely reported. Reporters Without Borders on Thursday said it had identified more than 40 serious violations of the rights of foreign journalists in Tibet and China since March10. And access to YouTube and mainstream media sites like the BBC, CNN, and Yahoo has also been restricted.

But there's no direct proof that anti-Tibetan cyberattacks are being directed by Chinese authorities.

"These attacks are sophisticated," said Greg Walton, who provides IT

support for Tibetans and researches Chinese computer espionage at the University of Sunderland in the United Kingdom. "We can only speculate where they're coming from. We can say the control servers are based in China. But these servers can just be stepping stones."

"Anything coming from China is not necessarily coming from the Chinese," said Marcus Sachs, director of the SANS Institute Internet Storm Center. "It could be coming from literally anyone from the planet."

Maarten Van Horenbeeck, a security researcher and SANS Institute Internet Storm Center handler, said in a Storm Center post Friday that politically motivated attacks have been reported at least since 2002 and that other communities and groups have been targeted, including Falun Gong and the Uyghurs.

"The attacks generally start with a very trustworthy looking e-mail, being spoofed as originating from a known contact, to someone within a community," Horenbeeck said. "In some cases, messages have also been distributed to mailing lists. These messages, however, contain malicious attachments." In early March, a computer security researcher at Sophos noticed different malware using Tibetan images to trigger an exploit.

A spokesperson for the FBI in Washington, D.C., confirmed that the agency had received information from the Save Darfur Coalition indicating that the group's e-mail accounts had been compromised by hackers who appear to be based in China and that the FBI is looking into the matter. The Save Darfur Coalition has been critical of China for "sponsoring the genocide in Darfur."

The FBI had no information to provide about attacks targeting Tibetan groups.

Sachs recounted how in 2001, following a collision between a U.S. Navy EP-3 reconnaissance plane and a People's Liberation Army jet, Chinese hackers attacked U.S. servers. "Best we could tell, there was no Chinese government involvement," he said.

Sachs believes the cyberattacks directed at Tibetan organizations are similarly the actions of Chinese hackers motivated by nationalism, without national direction.

The massive cyberattack on Estonia last year, in response to Estonia's decision to move a Russian war memorial, presents an analogous situation. While Russia's hand in the affair is easy to imagine, cybersecurity experts mostly see the attack as an act of nationalist zeal rather than coordinated, state-sponsored cyberwarfare.

Now that the Internet has evolved from a geeky curiosity to a shared transnational platform of economic, social, and political consequence, the question becomes, what kind of political response is appropriate for such attacks?

Were Canadians regularly shooting at the tires of U.S. trucks attempting to deliver goods into Canada, both the U.S. and Canadian governments would respond. Yet the information economy is not defended with the same enthusiasm as the real-goods economy.

Google, Microsoft, and Yahoo have tried to raise this issue by calling for the U.S. government to treat censorship as a trade barrier. To date, that hasn't happened.

In contrast to traditional political crises, where countries withdraw diplomats or impose sanctions to voice discontent, Sachs said, "In the cyberworld, we don't have centuries of diplomatic solutions. We're probably going to go through several decades of uncertainty about how to express displeasure."

--

Civiblog is an international initiative with the aim of giving voice to individuals and organizations involved in global civil society. We provide platforms and resources for NGOs, activists, dissidents and individuals at risk through the medium of blogging.

http://gregwalton.civiblog.org