UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
March 2012

Information Operations and Tibetan Rights in the Wake of Self-Immolations: Part I

KEY FINDINGS

This post is the first in a series of analyses that the Citizen Lab is preparing regarding the urgent and ongoing threat presented by information operations deployed against Tibetans and others who advocate for Tibetan rights and freedoms, including in Tibetan areas of China. The Citizen Lab is concerned with the apparent increase in the use of social engineering linked to the issue of self-immolation to target Tibetan activists with malware, as well as the reported increase in magnitude of information controls (in close coordination with more physical measures) utilized by the Chinese government in Tibetan areas.

Particularly in light of the upcoming March 10 anniversary of Tibetan Uprising Day, Citizen Lab urges all human rights organizations or others concerned with Tibetan rights to exercise vigilance concerning their use of information and communication technologies at this sensitive time, especially with respect to emails that reference self-immolation or anniversary-related activities.

BACKGROUND

In the 2011-2012 period, two significant factors have increased the stakes surrounding the issue of rights and freedoms of Tibetans. Those factors are the rise in the practice by Tibetans of self-immolation as a form of protest against government policies; and the rapidly approaching leadership transition that will take place at the 18th Party Congress of the Communist Party of China (CPC) in Fall 2012. The practice of self-immolation -- a controversial manifestation of Tibetan opposition to Chinese government policies -- has seriously undermined the assertions of the government that Tibetans benefit from and favor the policies of the CPC, drawing international attention to the issue. At the same time, the leadership transition has further incentivized the government to maintain stability at all costs and stamp out any perceived threat to CPC legitimacy.

Since 2009, it is estimated that 26 Tibetans have self-immolated, nearly all of whom died as a result. The first reports of self-immolation by Tibetan populations in China surfaced in February 2009, when a monk in Sichuan province set himself on fire outside of a monastery several days before the 50th anniversary of the Tibetan uprising. This event was followed by the March 2011 self-immolation of a second monk in Sichuan province on the third anniversary of protests at the Kirti monastery. By February 2012, the self-immolations expanded to include laypersons, when three herders in Seda county, Sichuan province, became the first non-clergy to commit the act. The self-immolations of the first female laypersons took place in early March 2012 with the deaths of a 19 year old student and a young widow in Ngaba county, Sichuan province.

The Chinese government's tone in its official response to the events has developed as the practice has became more widespread. Government response has ranged from outright denial to accusations the protests are led by organized crime and are a form of terrorism. Chinese Premier Wen Jiabao criticized the protesters as radicals attempting to undermine stability in the Tibet Autonomous Region. A spokesperson for China's top political advisory board most recently suggested that the Dalai Lama has incited the practice as an act of separatism and encouraged Tibetans to commit suicide, a claim contradicted by the Dalai Lama's previous statements. In sum, rather than confronting root issues of concern to Tibetans, government representatives have instead framed the incidents as the acts of criminals and the result of a plot by the Dalai Lama.

In this context, information operations[1] play a key role in the control or compromise of individuals voicing concern for Tibetan rights. Some of these operations are launched by and clearly attributable to the Chinese government. Others, such as targeted cyber attacks, involve more ambiguous attribution.

GOVERNMENT INFORMATION OPERATIONS

The Chinese authorities have taken a multifaceted approach to controlling the discontent, which includes not only an increase in the presence of military and law enforcement personnel in sensitive regions, but also media campaigns to discredit protesters and an information blackout that has cut off Internet access and mobile phone networks.[2] In response to the protests, Chinese authorities have reportedly flooded affected towns with paramilitary forces and riot police, establishing roadblocks as a means of restricting access to outside observers. Tibetan Buddhist pilgrims returning from a religious gathering in India were detained and interrogated, while government officials in Tibet have been threatened with disciplinary action should the protests continue.

In tandem with these physical measures, the government has taken overt steps to limit the electronic flow of information in the region as well. Since January 2012, Internet and mobile blackouts have been reported in predominantly Tibetan regions of China. Early reports from Sichuan province indicated that the towns of Serthar and Luhuo, sites of conflict in late January between Chinese security forces and protesters, had their telephone and Internet service severed. Reports citing the Global Times, a state-run newspaper, claimed that

Internet connections and mobile phone networks were cut for 50km surrounding the protest areas. The Global Times cited a local party official who confirmed that Internet access had been disrupted but denied that the self-immolations had occurred. Other reports have indicated that text messaging and Internet access were disrupted in Sichuan province and the Tibet Autonomous Region. Following a self-immolation on March 5, it was reported that the mobile phones of observers were confiscated to prevent news of the incident from spreading. Other reports have suggested that a number of Tibetan language blog sites hosted in China went offline in early February without explanation.

Meanwhile, Chinese authorities have continued a media campaign to discredit the protesters. State-owned media outlets have linked the protests to organized crime and blamed external forces and separatists for the conflict.

TARGETED CYBER ATTACKS

In addition to official government information controls, the Citizen Lab is highly concerned with the murky and more difficult-to-attribute targeted malware attacks launched against Tibetan rights advocates. Recent reports from the Tibetan community indicate that numerous malicious emails around the theme of self-immolation have been circulating among Tibetan organizations and activists. Human rights groups are often targeted by malware attacks that leverage issues and events of concern to particular communities to entice users in those communities to open malicious documents or click on links. The Citizen Lab has been tracking these kinds of attacks for some time (see Nobel Peace Prize, Amnesty HK and Malware; Human Rights and Malware Attacks; Targeted Malware Attack on Foreign Correspondents Based in China; "0day": Civil Society and Cyber Security).

In analyzing the recent spate of malicious emails referencing self-immolation, the Citizen Lab has found that the attackers use a variety of social engineering tricks and malware delivery mechanisms often observed in targeted attacks. The Citizen Lab presents a basic overview of its findings here, and will continue to release new and more detailed findings as it continues its research.

Social engineering techniques encountered in this analysis include:

- In several cases the attackers have re-purposed existing material from Tibetan activist groups, incorporating such material into the content of the malicious emails and attachments. For example, one malicious email contained a copy of a real post published by Students for a Free Tibet regarding participation in March 10 demonstrations, but with the addition of links to malicious Word and Excel documents.
- Other emails contained text from various news articles related to self-immolation, often taken from articles published the very same day the email was sent.

- The emails occasionally included benign images, for example of monks at a candlelight vigil, to entice the recipient to open the attachments.
- The malware was not always delivered through an attachment. Other tactics used by the senders were the inclusion of a link to a malicious document on a web server; and inclusion of links that appear to reference legitimate news sources, but in which the underlying link actually routes to a web page that exploits a Java vulnerability in order to infect the recipient's machine (a so-called "drive-by download").

Findings concerning the technical features of the malware analyzed in this analysis include:

- The most common vulnerability exploited in the samples the Citizen Lab has seen is CVE-2010-3333, in which an RTF document is given the file extension .doc so it opens in Microsoft Word and drops a malicious payload.
- When a malicious file is opened, it will typically drop a decoy file that is shown to the user while the payload executes in the background.
- Attackers have also made use of the Unicode right-to-left override technique to make an executable file appear to be a document in Windows Explorer.
- Attachments often come inside an archive (.zip or .rar file) to avoid detection by automated virus scans.

Additionally, it is important to note that Mac users are not immune to these threats. At least one attachment we have seen specifically targets Mac OS X, and the drive-by download checks which operating system the user is running and attempts to execute malware specific to the user's platform.

The Citizen Lab will continue its investigation of information operations and Tibetan rights, and will post further analysis as it becomes available at citizenlab.org.

RECOMMENDATIONS FOR DEFENDING AGAINST TARGETED CYBER THREATS

Steps individuals can take to reduce risk of exposure to malware include the following:

- Be vigilant concerning all e-mails, web links, and files, especially during sensitive times such as political anniversaries. In particular, carefully assess the authenticity of any such materials referencing sensitive subject matter, such as self-immolations or anniversary-related activities, or containing misspellings or unusual diction.
- Carefully examine the sender's email address. If the address uses an email account name that appears official, but originates from a common webmail provider (e.g. Gmail), or incorporates minor variations

from or unexpected characters than a typical address, consider it a spoofing attempt. Do not access any material included in that email without independently verifying that the actual person in question sent the email (do not reply to the same email address from which the email originates — use telephone calls or research the official email address).

- Never open unexpected or unsolicited attachments. If the attachment is not essential to your work or represents information you can obtain elsewhere (such as through an online search for a particular report or issue), immediately delete it. If you are using Gmail, you can click “View” to view some attachments in your web browser instead of downloading the file to your computer. All file types may contain malware, but be especially wary of .exe, .scr, .zip, and .rar files. If it is essential that you open the file, try to independently confirm with the actual person who appears to have sent it that the file is legitimate. Additionally, running the file through https:/www.virustotal.com/ may help to identify files containing malware (though it will not catch zero-day exploits). To perform such a scan, drag or copy the file to your desktop without opening it, and then upload to the virustotal website. The website will provide a summary of results of the scan.
- Never click on unverified links. As with attachments, if the link is not essential to your work or represents information you can obtain elsewhere (such as through an online search), immediately delete it. Keep in mind that hyperlinks that appear to lead to legitimate sites, may in fact mask an underlying malicious web link. In most email programs, if you hover over a hyperlink without clicking, it will show you the actual link as a tooltip (text that briefly appears next to the mouse cursor), or, in the case of webmail, in the status bar of your browser. Suspicious links might have an IP address instead of a domain (e.g. http://10.0.3.10/something.html instead of http://example.com/something.html) or the URL may not match the website to which you expect it to link. If the text of the link in the email does not match the underlying link, there is a good chance the linked page is malicious.
- Keep your computer’s operating system, applications and anti-virus program up to date and ensure you have the latest security updates and patches.
- Be aware of mobile malware. More and more malware released nowadays is designed for mobile phones. Do not download apps that you don’t need, as many apps available in open markets contain malware. There are also projects developing applications to help mobile users protect their communications and personal data from intrusion and monitoring.

If you are part of a human rights organization and are interested in participating in the Citizen Lab’s ongoing study of targeted cyber threats, please contact us at hrthreats[AT]citizenlab.org

FOOTNOTES

[1] While the term “information operations” is often associated with military action, use of the term here is meant to refer to all aspects of information-related capabilities deployed against targeted entities or individuals, and is not limited to operations linked to the military. Such operations may include computer network exploitation/attacks, sabotage, surveillance, espionage, or psychological operations incorporating new media and technology to influence public sentiment and shape the communications space.

[2] This is not the first time the severing of Internet access has been used as a form of information control during civil unrest in China. In 2008, following unrest that broke out in Tibet after protests marking the anniversary of the 1959 Tibetan Uprising, Chinese authorities restricted media coverage of the incidents and limited the spread of related Internet content. It has been reported that these information controls included the blocking of content related to the event, the confiscation of mobile phones and the shutdown of cellular networks. Additionally, in 2009, following riots between Uyghur and Han populations in Urumqi, Chinese authorities shut down Internet service in the Xinjiang Uyghur Autonomous Region. The government asserted that the riots had been organized through the Internet and text messaging, and the blackout was not lifted until May 2010.