Vietnam's 'cyber troops' take fight to US, France

January 20 2014, by Chris Brummitt

In this May 14, 2013 photo, three young Vietnamese women use a laptop and smart phones to go online at a cafe in Hanoi, Vietnam. Vietnamese pro-democracy activists and bloggers are battling a gathering campaign of blocking, hacking and spying by a shadowy pro-government army of cyber warriors. Although they can't prove it, activists and analysts strongly suspect the Vietnamese state is involved in the campaign, which is hampering the country's democracy movement. (AP Photo/Na Son Nguyen, File)

Working on her blog in California one day, Vietnamese democracy

activist Ngoc Thu sensed something was wrong. It took a moment for a keystroke to register. Cut-and-paste wasn't working. She had "a feeling that somebody was there" inside her computer. Her hunch turned out to be right.

A few days later, her personal emails and photos were displayed on the blog, along with defamatory messages. She couldn't delete them; she was blocked out of her own site for several days as her attackers kept posting private details.

"They hurt me and my family. They humiliated us, so that we don't do the blog anymore," said Thu, who is a U.S citizen. She has resumed blogging, but now the Vietnamese government is blocking her posts.

Activists and analysts strongly suspect Hanoi was involved in that attack and scores of others like it.

They say a shadowy, pro-government cyber army is blocking, hacking and spying on Vietnamese activists around the world to hamper the country's pro-democracy movement.

IT experts who investigated last year's attack on Thu said the hackers secretly took control of her system after she clicked on a malicious link sent to her in an email. By installing key-logging software, the hackers were able to harvest passwords, gaining access to her private accounts.

Subsequent investigation also found that an upgraded version of the malicious software, sent by the same group, was emailed to at least three other people: a British reporter for the Associated Press reporter based in Hanoi; a France-based Vietnamese math professor and democracy activist; and an American member of the Electronic Frontier Foundation, an online activist group, living in the United States. None of the three clicked the link.

It appears to be the first documented case of non-Vietnamese being attacked by a pro-government hacking squad that had already conducted attacks well beyond the borders of this Southeast Asian nation. Its actions would appear to violate the law in the United States at least.

"You see campaigns being waged against Vietnamese voices of dissent in geographically disparate regions. Now we have seen an escalation against people who report on those voices," said Morgan Marquis-Boire, a University of Toronto researcher and online privacy activist who dissected the malware and published the findings with the EFF. "It's unlikely that this is the work of an opportunist individual."

Suspicion of state involvement is based in part on the fact that attackers have spent tens of thousands of dollars hiring servers around the world from which to launch attacks, often changing them after a few days. This is because the attackers know activists will ask service providers to take them down, said Dieu Hoang, an Australian computer engineer who, along with several other activists, works to help defend the Vietnamese activists online.

Attempts to monitor and harass dissidents online mirror the government's efforts to suppress them on the ground, where activists report persistent and occasionally violent harassment by state agents. The state convicted at least 63 bloggers and other nonviolent democracy activists in 2013 of criminal offenses, according to Human Rights Watch.

Vietnam is by no means unique in seeking to spy on electronic communications, as recent revelations about the actions of the National Security Agency in the United States demonstrate. But its activities are of special concern because of its human rights record in general.

Asked to comment on suspicions of state involvement in targeted

surveillance, as well as the attack on the AP reporter, the Vietnamese government gave this brief statement: "Vietnam shares the attention of other countries in ensuring Internet security and is willing to cooperate with other countries in fighting high-tech crimes in general and Internet crimes in particular."

In this May 14, 2013 file photo, a Vietnamese man uses a 3G device to get online at a cafe in Hanoi, Vietnam. Vietnamese pro-democracy activists and bloggers are battling a gathering campaign of blocking, hacking and spying by a shadowy pro-government army of cyber warriors. Although they can't prove it, activists and analysts strongly suspect the Vietnamese state is involved in the campaign, which is hampering the country's democracy movement. (AP Photo/Na Son Nguyen, File)

Suppressing online dissent in Vietnam is becoming more difficult because of soaring Internet usage. Close to 40 percent of the country's

90 million people have Internet access, and because Vietnam has been less effective than China in restricting that access, many people are viewing uncensored news. Dissidents can network and publicize their activities—and acts of state repression—with comparative ease.

Security researchers have found hints of how Hanoi may be dealing with the challenge.

In 2010, Google and McAfee alleged that that malicious software had been used to spy on tens of thousands of Vietnamese web users. McAfee said the perpetrators of the attacks "may have some allegiance" to the country's government. Last year, researchers led by Marquis-Boire, who also works for Google as a security engineer, uncovered evidence suggesting a spyware suite called FinFisher was being used to track activists' mobile communications inside Vietnam.

The government, through state media, has admitted to blocking thousands of "bad, poisonous web sites and blogs," and its sites have come under attack, presumably from dissident sympathizers. Ho Quang Loi, propaganda chief of Hanoi's Communist Party, said last year it employed 900 people to counter online criticism.

The attack on Thu's blog showed how hacking and blocking can work as a one-two punch to knock out criticism.

The blog, named "Ba Sam," is one of the best-known dissident publications. It carries news, views, videos and photos from and about Vietnam of the kind that state media would never touch. After the blog was hacked, it took Thu a week to regain control, move it to a new address and put it back online.

Within weeks, authorities in Vietnam began blocking it to web users inside the country. To view it now, people inside Vietnam have to use a

proxy server, a relatively common technique for censorship evasion but one that requires some knowhow. This means fewer people are seeing it.

Thu said her page views are down significantly, and that she shut down her popular comments sections because of an organized campaign of abuse and spamming.

"It became too much trouble," she said. "They sent me threatening messages saying, 'I'm going to visit you in California.'"

Hacking a site and blocking it later is a known tactic, said Hoang, the Australian.

"Defacing and defaming is done by a hidden force unofficially," he said. "Blocking is done by the official force."

The malware sent to Thu and the others was undetected by almost all the commercial anti-virus software experts used on it. The emails accompanying the malicious link sent to the AP reporter exhibited some thought and degree of targeting: one purported to be from Human Rights Watch, the other from Oxfam. The emails were sent in November and December of last year.

Proving a Vietnamese state hand in the attacks is hard.

"As a general rule, pinpointing the actor behind is difficult. It is much more difficult than taking the malware apart," said Eva Galperin, the EFF activist who received the link. "I think suspicion is warranted, but I would stop short of saying that I know the Vietnamese government responsible."

While some overseas activist groups run courses in cyber security for their members, the hackers appear to be winning the battle, Hoang said.

"In terms of time and effort and headcount and money, we can't even compare to them. After a while we will be worn out. They slow the people down, make them frustrated, make them scared. They are going to make less and less people put out their message."

More information: A link to the EFF report on the attacks: www.eff.org/deeplinks/2014/01/ … alware-gets-personal