DENIAL OF SERVICE

CYBERATTACKS BY THE VIETNAMESE GOVERNMENT

Michel Tran Duc and Duy Hoang
Viet Tan - www.viettan.org/en

April 27, 2010

DENIAL OF SERVICE | FROM FIREWALLS TO CYBERATTACKS

FROM FIREWALLS TO CYBERATTACKS

In the early days of the web–prior to social networks and before there were 25 million Vietnam internet users–the Government of Vietnam exercised online censorship by blocking politically sensitive websites. The firewall prevented internet users in Vietnam from accessing outside websites operated by the diaspora that discussed democracy, religious freedom or news critical of the Hanoi regime.

As web blogs became popular, facilitating the participation of Vietnamese in online political discourse, authorities resorted to harassing and even jailing prominent bloggers. Several renowned bloggers such as Dieu Cay and Tran Khai Thanh Thuy are currently imprisoned for their peaceful expression. Beginning in 2008, authorities extended the legal pretext for censoring blogs and monitoring the internet. (See *Vietnam's Blogger Movement: A Virtual Civil Society in the Midst of Government Repression* by Viet Tan, April 2009).

In recent months, the government has stepped up efforts to restrict internet freedom by ordering local internet service providers to block access to Facebook and other social networking sites.

In their pursuit for even stricter online censorship, Vietnamese authorities launched unprecedented cyberattacks against websites based *outside* of the country and employed malicious software to penetrate the computers of webmasters and human rights activists.

We can confirm that the attacks originated from Vietnam based on Internet Protocol (IP) addresses obtained by Viet Tan and other organizations that were victimized. Investigations by Google and computer security firm McAfee further confirm that entities inside Vietnam orchestrated the cyber attacks.

Given the scale and coordination of the attacks, only the Vietnamese authorities have the capability, along with the desire, to take down opposition voices. Coinciding with the repression in cyberspace, the government launched an offline crackdown against peaceful expression, detaining many of the bloggers and activists whose sites were affected. Since October 2009, over 20 activists have been sentenced to jail for their peaceful political advocacy.

DENIAL OF SERVICE | ENVIRONMENTAL OPPOSITION PROMPTS MAJOR HACKING

ENVIRONMENTAL OPPOSITION PROMPTS MAJOR HACKING

Vietnam's largest movement for civil action to date coalesced over concern for the environmental and security risks of mining bauxite, a mineral used to produce aluminum, in the ecologically sensitive Central Highlands. In March 2009, leading academics initiated a petition calling on the government to reconsider its bauxite policy, especially the involvement of a Chinese state-owned company not known for its environmental stewardship. Within months thousands of concerned citizens had signed the petition.

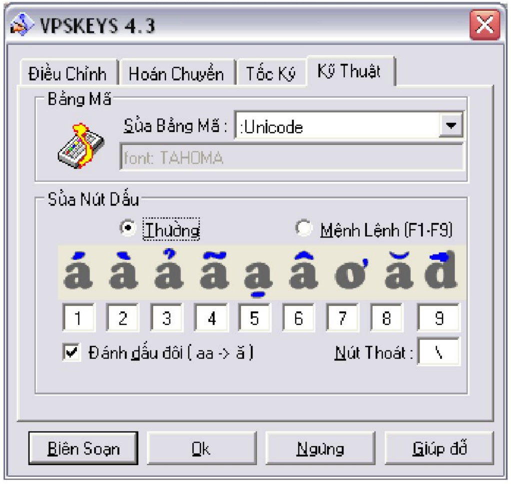
> Bauxitevietnam.info's role in organizing a civic movement was highlighted by Al-Jazeera.

The organizers created a website named Bauxite Vietnam (www.bauxitevietnam.info), hosted on a server in France, which attracted nearly 20 million hits by December 2009. Faced with this new challenge, authorities sought to shutdown the site and divide and intimidate the organizers.

Through massive distributed denial of service attacks (DDoS) in December 2009 and January 2010, authorities crashed bauxitevietnam.info. One of the ways they generated the computing capacity to assault Bauxite Vietnam and disguise their role was by infecting the computers of many unwitting users. Hackers switched a popular software for inputting Vietnamese-characters written by the California-based Vietnamese Professionals Society (VPS), called VPSKeys, with a malicious version that took over people's computers, according to McAfee and VPS.

To get users to download the malware, given the name W32/Vulcanbot by McAfee, a fake email from VPS was circulated asking people to download the "new" (malware) version of VPSKeys.

> VPSKeys is a popular software for inputting Vietnamese language characters.



Sửa Bảng Mã : :Unicode

font: TAHOMA

● Thường ○ Mệnh Lệnh (F1-F9)

☑ Đánh dấu đôi (aa -> ă)

Nút Thoát : \

Once users installed the malicious software their computer became part of a botnet controlled by the hacker. Infected computers (a.k.a. zombies) would phone back to a dynamic Domain Name System (DNS) to receive instructions, one of which was to perform a denial of service attack on bauxitevietnam.info. According to McAfee, the botnet was primarily controlled from IP addresses in Vietnam.

These attacks happened around the same time as the China/Google attack, causing Google to be suspicious and work with McAfee to analyze the botnet. The two companies publicized their discovery of the VPSKeys malware through blog posts on March 30, 2010. While the China affair prompted their investigation, both McAfee and Google have ruled out that the Vietnam incident was related to events in China.

The hacking of bauxitevietnam.info was part of a larger, organized effort to squash the environmental movement. In December 2009, forged emails of petition organizers were widely circulated online. These emails sought to sow division by accusing fellow organizers with various improprieties. One email under the name of Pham Toan, a co-founder of Bauxite Vietnam, announced that he was quitting the movement. Pham Toan subsequently gave radio interviews on BBC and RFI confirming that he never wrote such an email.

In January 2010, security police repeatedly detained Nguyen Hue Chi, Pham Toan and other participants in the bauxite movement as a means of intimidation. Bauxite Vietnam currently operates on blogspot.com and wordpress.com which are much harder for hackers to shut down. It has launched three separate websites (boxitvn.net, boxitvn.org and boxitvn.info) which have been under regular attack since January and are firewalled in Vietnam.

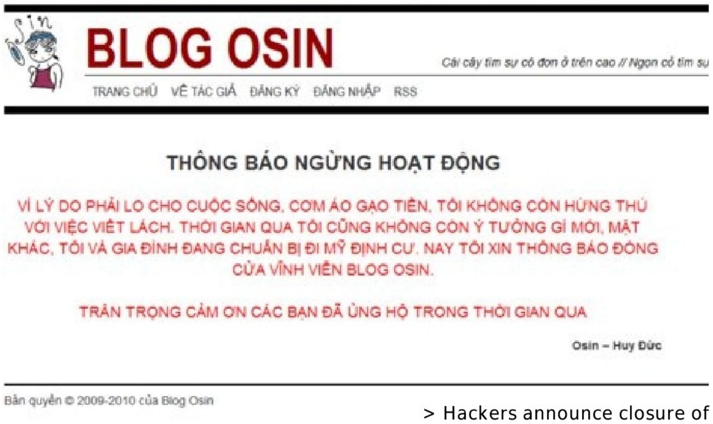
WE EXPRESS TO FREE
THE OPPRESSED
2010 International Women's Day
FreeThuyNhanNghien.multiply.com

> Viet Tan is actively campaigning for the release of three prominent Vietnamese women cyber activists.

> Blogger Dieu Cay called for a boycott of the Beijing Olympic torch relay.

LEADING POLITICALLY-ORIENTED SITES TARGETED

Beginning in December 2009, numerous Vietnamese-language websites hosted on servers outside of Vietnam either had their admin passwords stolen or suffered massive distributed denial of service attacks. These sites included personal blogs (Osin, Vang Anh) and discussion forums (x-Cafe, Dan Luan, Talawas, DCVOnline) popular among readers in Vietnam.



THÔNG BÁO NGỪNG HOẠT ĐỘNG

VÌ LÝ DO PHẢI LO CHO CUỘC SỐNG, CƠM ÁO GẠO TIỀN, TÔI KHÔNG CÒN HỨNG THÚ VỚI VIỆC VIẾT LÁCH. THỜI GIAN QUA TÔI CŨNG KHÔNG CÒN Ý TƯỞNG GÌ MỚI, MẶT KHÁC, TÔI VÀ GIA ĐÌNH ĐANG CHUẨN BỊ ĐI MỸ ĐỊNH CƯ. NAY TÔI XIN THÔNG BÁO ĐÓNG CỬA VĨNH VIỄN BLOG OSIN.

TRÂN TRỌNG CẢM ƠN CÁC BẠN ĐÃ ỦNG HỘ TRONG THỜI GIAN QUA

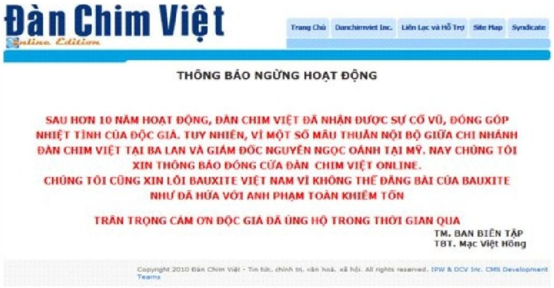
Osin – Huy Đức

Bản quyền © 2009-2010 của Blog Osin

> Hackers announce closure of Blog Osin.

Journalist Huy Duc, who operates the Osin blog, had been targeted by authorities for over a year. Under government pressure, his employer at a state-owned newspaper was forced to fire him in June 2009 after he blogged about the inhumanity of the Berlin Wall. When hackers took over his site in January 2010, they posted a fake good-bye note from Osin to readers. The demeaning announcement said Osin was giving up blogging because he "ran out of new ideas" and would focus on "personal pursuits, food and clothing."

A fictitious note also appeared on DCVOnline.net after this news and discussion site was hacked. The note claimed the site was closing due to internal conflicts and apologized for not publishing an article purportedly submitted by one of the Bauxite Vietnam organizers.



THÔNG BÁO NGỪNG HOẠT ĐỘNG

SAU HƠN 10 NĂM HOẠT ĐỘNG, ĐÀN CHIM VIỆT ĐÃ NHẬN ĐƯỢC SỰ CỔ VŨ, ĐÓNG GÓP NHIỆT TÌNH CỦA ĐỘC GIẢ. TUY NHIÊN, VÌ MỘT SỐ MÂU THUẪN NỘI BỘ GIỮA CHI NHÁNH ĐÀN CHIM VIỆT TẠI BA LAN VÀ GIÁM ĐỐC NGUYỄN NGỌC OÁNH TẠI MỸ. NAY CHÚNG TÔI XIN THÔNG BÁO ĐÓNG CỬA ĐÀN CHIM VIỆT ONLINE.
CHÚNG TÔI CŨNG XIN LỖI BAUXITE VIỆT NAM VÌ KHÔNG THỂ ĐĂNG BÀI CỦA BAUXITE NHƯ ĐÃ HỨA VỚI ANH PHẠM TOÀN KHIÊM TỐN

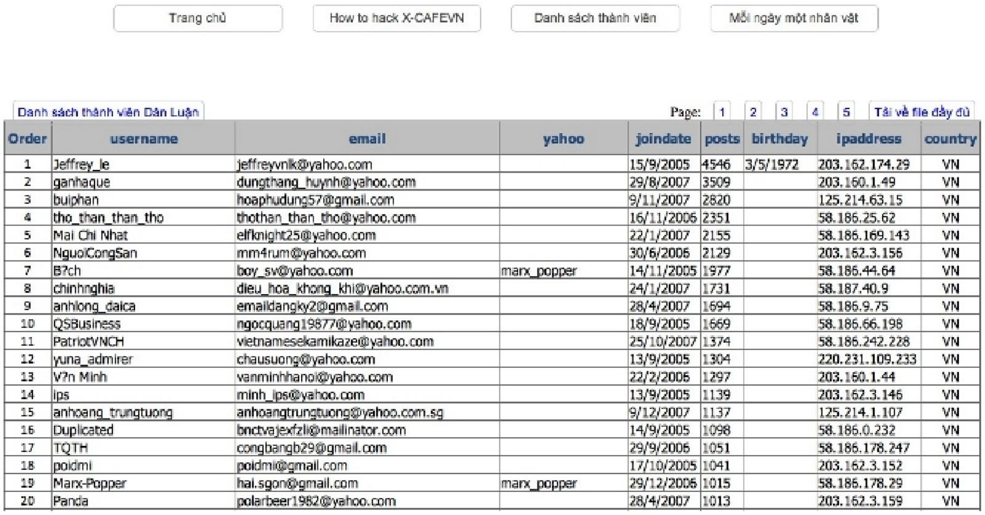
TRÂN TRỌNG CẢM ƠN ĐỘC GIẢ ĐÃ ỦNG HỘ TRONG THỜI GIAN QUA

TM. BAN BIÊN TẬP
TBT. Mạc Việt Hồng

Copyright 2010 Đàn Chim Việt - Tin tức, chính trị, văn hoá, xã hội. All rights reserved. IPW & DCV Inc. CMS Development Teams

> Hackers leave a note on DCVOnline.net.

In an effort to intimidate the in-country and overseas Vietnamese internet community, hackers posted online the entire user database of the x-cafevn.org discussion forum. The login name, email, location and IP address of over 19,000 users were publicly displayed. In addition, alleged profiles of the admins and various activists associated with x-cafe.org were posted on .www.x-cafevn-db.info



Order	username	email	yahoo	joindate	posts	birthday	ipaddress	country
1	Jeffrey_le	jeffreyvnlk@yahoo.com		15/9/2005	4546	3/5/1972	203.162.174.29	VN
2	ganhaque	dungthang_huynh@yahoo.com		29/8/2007	3509		203.160.1.49	VN
3	buiphan	hoaphudung57@gmail.com		9/11/2007	2820		125.214.63.15	VN
4	tho_than_than_tho	thothan_than_tho@yahoo.com		16/11/2006	2351		58.186.25.62	VN
5	Mai Chi Nhat	elfknight25@yahoo.com		22/1/2007	2155		58.186.169.143	VN
6	NguoiCongSan	mm4rum@yahoo.com		30/6/2006	2129		203.162.3.156	VN
7	B?ch	boy_sv@yahoo.com	marx_popper	14/11/2005	1977		58.186.44.64	VN
8	chinhnghia	dieu_hoa_khong_khi@yahoo.com.vn		24/1/2007	1731		58.187.40.9	VN
9	anhlong_daica	emaildangky2@gmail.com		28/4/2007	1694		58.186.9.75	VN
10	QSBusiness	ngocquang19877@yahoo.com		18/9/2005	1669		58.186.66.198	VN
11	PatriotVNCH	vietnamesekamikaze@yahoo.com		25/10/2007	1374		58.186.242.228	VN
12	yuna_admirer	chausuong@yahoo.com		13/9/2005	1304		220.231.109.233	VN
13	V?n Minh	vanminhhanoi@yahoo.com		22/2/2006	1297		203.160.1.44	VN
14	ips	minh_ips@yahoo.com		13/9/2005	1139		203.162.3.146	VN
15	anhoang_trungtuong	anhoangtrungtuong@yahoo.com.sg		9/12/2007	1137		125.214.1.107	VN
16	Duplicated	bnctvajexfzli@mailinator.com		14/9/2005	1098		58.186.0.232	VN
17	TQTH	congbangb29@gmail.com		29/9/2006	1051		58.186.178.247	VN
18	poidmi	poidmi@gmail.com		17/10/2005	1041		203.162.3.152	VN
19	Marx-Popper	hai.sgon@gmail.com	marx_popper	29/12/2006	1015		58.186.178.29	VN
20	Panda	polarbeer1982@yahoo.com		28/4/2007	1013		203.162.3.159	VN

> Private user information from x-cafevn.org posted online.

According to people knowledgeable with the situation, these profiles consisted of assorted real and fake details. The objective was to make the web community believe that Hanoi's intelligence agents working with hackers could obtain dossiers on virtually any Vietnamese activist or internet user. Hackers got access to x-cafevn.org by using malware to steal the password of an admin for the site.

HACKER ATTACKS AGAINST VIET TAN

The Viet Tan website routinely experiences DoS and DDoS attacks on a small to moderate scale.

On April 30, 2009, viettan.org suffered a major denial of service attack. We believe hackers from Vietnam employed the xFlash attack method. They hacked into several other websites and installed a program named vnattackerpop.swf. Visitors to those sites unwittingly ran the script on their computers and subsequently attacked viettan.org. During a five day period, the viettan.org server was inundated with tens of millions of requests.

Viet Tan contacted the sites that contained the attacking script and requested its removal. The denial of service attacks consequently ceased. The timing of the attack had a political significance. April 30th marks the fall of Saigon to communist forces.

The viettan.org server also experienced numerous attempts of unauthorized entry and brute-force password cracking of internal email accounts. These attacks happened on a frequent basis. After web administrators blocked the IP addresses from where these attempts orginiated from, hackers would simply switch to a different set of IP addresses.

DATE OF ATTACK	SITE	CONTENT	SERVER LOCATION
Feb. 2010 - present	www.blogosin.org	Blog	United States
Jan. 2010 - present	www.doi-thoai.com	News	United States
Jan. 2010 - present	www.caotraonhanban.com	Pro-democracy	United States
Jan. 2010	www.danluan.org	News and discussion	United States
Jan. 2010	vanganh.multiply.com	Blog	United States
Jan. 2010	www.x-cafevn.org	News and discussion	United States
Jan. 2010	www.dcvonline.net	News and discussion	United States
Dec. 2009 - Jan. 2010	www.talawas.org	Commentary and discussion	United States
Dec. 2009 - Jan. 2010	www.bauxitevietnam.info	Environmental opposition	France
Apr., May, Dec. 2009	www.viettan.org	Pro-democracy	France

> Partial list of cyberattacks against websites based outside of Vietnam.

Viettan.org is generally firewalled in Vietnam. Occasionally, internet users in Vietnam have reported that the firewall had been lifted and they could access the Viet Tan website. This opening of the gates usually coincides with a denial of service attack from Vietnam–one sure sign that the hacking attacks are sponsored by Vietnamese government authorities

Besides targeting Viet Tan's computing infrastructure, hackers routinely targeted Viet Tan members directly by emailing malware disguised as normal documents. A few Viet Tan members have had their computers affected with malware allowing hackers to obtain working email correspondences. Recently, hackers published these email messages on www.x-cafevn-db.info, a site boasting their exploits.

POLICY RECOMMENDATIONS

1. *Condemn cyberattacks by Vietnamese authorities*

By targeting websites and internet users outside of Vietnam, the Hanoi government is no longer restricting the internet freedom of just Vietnamese citizens. It is also infringing on the rights and privacy of netizens around the world. The cyberattacks and theft of user data may also violate national laws. Entities within Vietnamese behind these illegal activities must be held to account.

2. *Call on the Vietnamese government to respect internet freedom*

The Vietnamese government must repeal laws that criminalize peaceful expression. In particular, Decree No. 97/2008/ND-CP on management of blogs and the Ministry of Public Security's order shutting down Facebook are inconsistent with international human rights conventions to which Vietnam is a signatory. Internet censorship is also contrary to the Vietnamese government's stated aim of developing a knowledge-based economy.

3. *Demand that the Vietnamese government release imprisoned bloggers and cyber activists*

You can bring public attention to the cases of Vietnamese bloggers and activists who have been imprisoned for their peaceful expression. Express your solidarity with these prisoners of conscience and provide support to their families.

4. *Promote knowledge of internet security and circumvention methods*

You can also assist internet users to circumvent the Vietnam's government firewalls and protect against hacking attacks through technical, financial and educational assistance. This knowledge can help Vietnamese bloggers to be more effective investigative journalists, human rights defenders and grassroots organizers.

VIET TAN | HUMAN RIGHTS FOR VIETNAM

About Viet Tan

The mission of Viet Tan is to overcome dictatorship, build the foundation for a sustainable democracy, and demand justice and human rights for the Vietnamese people through a nonviolent struggle based on civic participation.

How to Get Involved

Support Viet Tan's current campaigns and let us know if you would like to participate in the next Viet Tan activity in your area.

Visit our website, join our mailing list and help spread information about our activities and the situation in Vietnam. You can also follow us on Twitter and Facebook.

We welcome new members and supporters who wish to contribute to the change they want to see in Vietnam.

www.viettan.org/en | www.facebook.com/vt4democracy | www.twitter.com/viettan

www.viettan.org/en