DENI DE SERVICES

LES CYBER-ATTAQUES DU GOUVERNEMENT VIETNAMIEN

Michel Tran Duc et Duy Hoang
Viet Tan - www.viettan.org/fr

DU PARE-FEU AUX CYBER-ATTAQUES

Aux débuts du web - avant la naissance des réseaux sociaux et avant que le Vietnam ne compte 25 millions d'internautes - le gouvernement vietnamien exerçait la censure en ligne en bloquant les sites politiquement sensibles. Le pare-feu empêchait les internautes au Vietnam d'accéder aux sites Web basés à l'étranger et gérés par de la diaspora, qui traitent de la démocratie, de la liberté religieuse ou des informations critiques envers le régime de Hanoi.

Au fur et à mesure que les blogs deviennent populaires, ce qui facilite la participation des Vietnamiens aux discussions politiques en ligne, les autorités recourent au harcèlement voire à l'emprisonnement des blogueurs les plus connus. Plusieurs blogueurs de renom tels que Dieu Cay et Tran Khai Thanh Thuy sont actuellement emprisonnés pour leur expression pacifique. Depuis le début 2008, les autorités ont élargi le recours au système judiciaire pour censurer les blogs et surveiller Internet. (Voir Le Mouvement des Blogueurs au Vietnam : une société civile virtuelle au milieu de la répression gouvernementale de Viet Tan, avril 2009).

Ces derniers mois, le gouvernement a intensifié ses efforts pour restreindre la liberté d'Internet, en ordonnant aux fournisseurs d'accès à Internet de bloquer l'accès à Facebook et d'autres sites de réseau social.

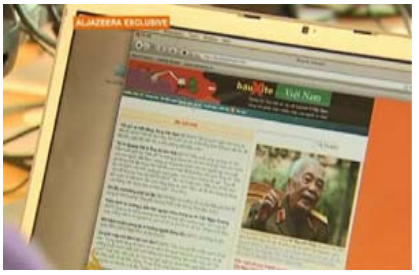
Dans leur volonté de censurer encore plus les activités en ligne, les autorités vietnamiennes ont lancé des cyber-attaques sans précédent contre des sites Internet basés à l'extérieur du pays et utilisent des logiciels malveillants pour s'introduire dans les ordinateurs des webmasters et des militants des droits de l'homme.

En se basant sur les adresses IP (Internet Protocol) recueillies par Viet Tan et d'autres organisations victimes, nous pouvons affirmer que les attaques viennent du Vietnam. Les enquêtes menées par Google et McAfee, l'éditeur d'anti-virus, confirment en outre que des entités à l'intérieur du Vietnam ont orchestré les cyber-attaques.

Étant donné l'ampleur et la coordination des attaques, seules les autorités vietnamiennes ont la capacité, et la volonté, de s'en prendre aux opposants politiques. Concomitamment à la répression dans le monde virtuel, le gouvernement a lancé une vague de répression contre l'expression pacifique dans le monde réel, détenant de nombreux blogueurs et militants dont les sites ont été visés. Depuis octobre 2009, plus de 20 militants ont été condamnés à la prison ferme pour leurs plaidoyers politiques pacifiques.

L'OPPOSITION ENVIRONNEMENTALE MOTIVE LES ATTAQUES

A ce jour au Vietnam, le plus grand mouvement d'action civique rassemble des gens préoccupés par l'environnement et les risques de sécurité liés à l'extraction de la bauxite, un minerai utilisé pour produire de l'aluminium, dans les hauts plateaux du centre, une région écologiquement sensible. En mars 2009, d'éminents universitaires ont lancé une pétition appelant le gouvernement à revoir sa politique d'extraction de la bauxite, en particulier la participation d'une société d'État chinoise qui n'est pas connue pour son respect de l'environnement. Des milliers de citoyens inquiets ont signé la pétition en quelques mois.

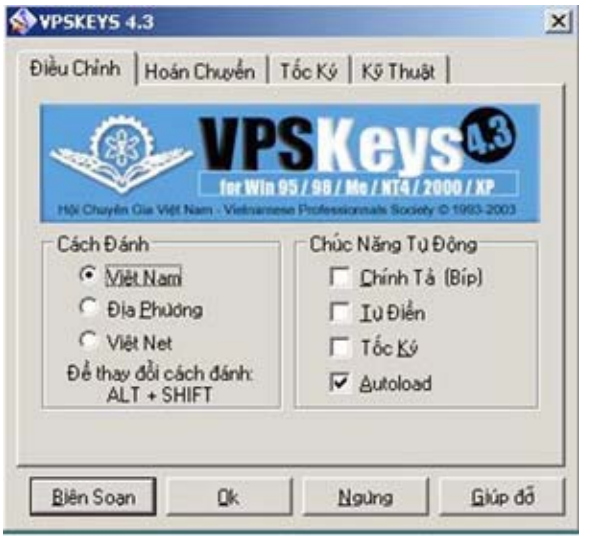


➢Al Jazeera a souligné le rôle de VietnamBauxite.info dans l'organisation des protestations populaires.

Les organisateurs du mouvement ont créé un site Web appelé Bauxite Vietnam (www.bauxitevietnam.info), hébergé sur un serveur en France, qui a attiré près de 20 millions de visiteurs en décembre 2009. Face à cette nouvelle forme de contestation, les autorités ont cherché à fermer le site et en divisant et en intimidant les organisateurs.

Via une attaque massive de déni de service distribué (DdoS – Distributed Denial of Services) en décembre 2009 et janvier 2010, les autorités ont fait crasher le site bauxitevietnam.info. Une des méthodes utilisées a été de prendre le contrôle de nombreuses machines à l'insu de leurs propriétaires pour attaquer Bauxite Vietnam et masquer leur rôle. Des hackers ont piraté le logiciel populaire VPSKeys, un logiciel gratuit d'écriture des caractères vietnamiens, édité par l'Association des Professionnels Vietnamiens (Vietnamese Professionals Society – VPS) basée en Californie, pour y introduire un logiciel malveillant permettant la prise de contrôle à distance des ordinateurs infectés, selon McAfee et VPS.

Pour inciter les utilisateurs à télécharger le logiciel virusé baptisé W32/Vulcanbot par McAfee, un faux courriel de l'association VPS a été adressé à certaines personnes les informant d'une « mise à jour du logiciel VPSKeys » et leur demandant de télécharger la « nouvelle » (fausse) version de VPSKeys.



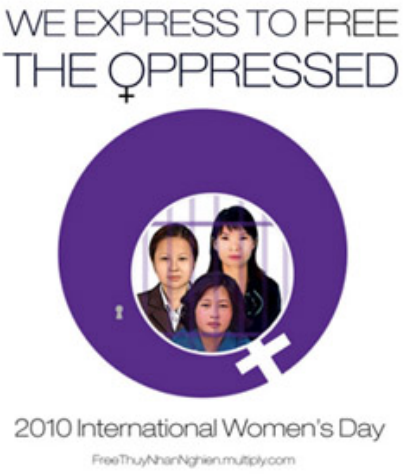
➢VPS Keys est un populaire logiciel libre pour écrire des caractères vietnamiens.

Une fois que les utilisateurs ont installé le logiciel malveillant, leur ordinateur fait partie d'un botnet (réseau de machines) contrôlé par les pirates. Les ordinateurs infectés (appelés zombies) contactent un système de noms de domaine (Domain Name System - DNS) dynamique pour recevoir des instructions, dont l'une d'entre elles consiste à lancer une attaque par le déni de service sur le site bauxitevietnam.info. Selon McAfee, le botnet est principalement télécommandé à partir d'adresses IP basées au Vietnam.

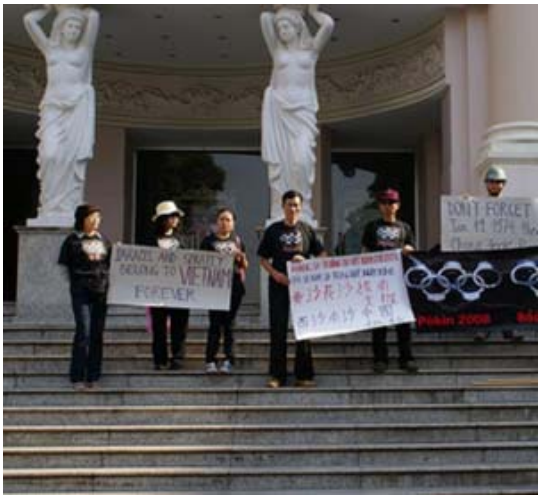
Ces attaques ont eu lieu autour de la même période que l'attaque sur Google en Chine, suscitant la méfiance de Google et poussant le géant d'Internet à travailler avec McAfee pour analyser le botnet. Le 30 mars 2010, les deux sociétés ont rendu public sur blog leur découverte du malware W32/Vulcanbot. Mais tant McAfee que Google ont exclu que l'incident avec le Vietnam soit lié à l'affaire en cours avec la Chine.

Le piratage de bauxitevietnam.info fait partie d'une action plus vaste organisée pour réduire au silence le mouvement écologiste. En décembre 2009, des faux e-mails des organisateurs de la pétition ont été largement diffusés sur internet. Ces courriels ont cherché à semer la discorde en accusant d'autres meneurs du mouvement de diverses irrégularités. Ainsi, un e-mail au nom de Pham Toan, un des co-fondateurs de Bauxite Vietnam, annonçait qu'il quittait le mouvement. Le vrai Pham Toan a ensuite donné des interviews radio sur la BBC et RFI confirmant qu'il n'a jamais écrit un tel courriel.

En janvier 2010, à plusieurs reprises, la police a interpellé Nguyen Hue Chi, Pham Toan et d'autres participants du mouvement de la bauxite pour les intimider. Les administrateurs du site ont tenté de relancer le portail d'information sur trois sites distincts (boxitvn.net, boxitvn.org et boxitvn.info). Tous trois ont été attaqués et un pare-feu empêche les internautes au Vietnam d'y accéder. Bauxite Vietnam est désormais hébergé sur blogspot.com et wordpress.com qui sont beaucoup plus difficile à attaquer pour les pirates.



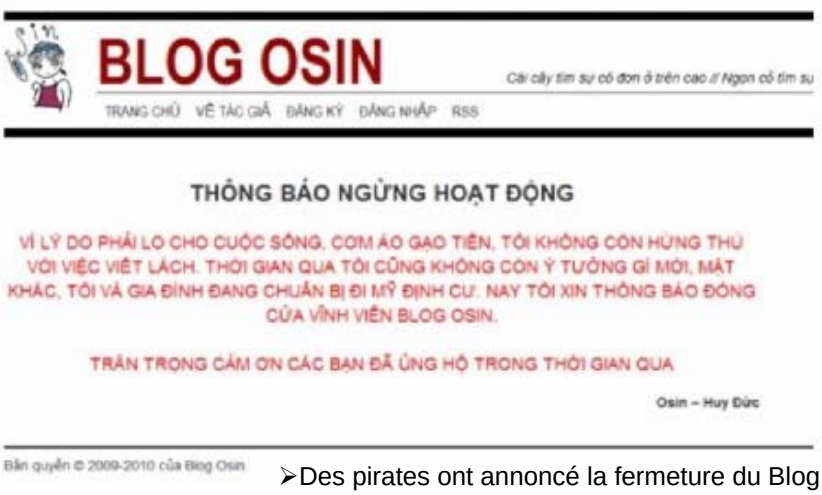
➢Viet Tan fait campagne pour la libération des militantes vietnamiennes pour la démocratie.



➢Le blogueur Dieu Cay a appelé au boycott du relais de la flamme olympique en 2008.

LES PRINCIPAUX SITES À ORIENTATION POLITIQUE CIBLÉS

Depuis décembre 2009, de nombreux sites en langue vietnamienne hébergés sur des serveurs à l'extérieur du Vietnam, soit ont vu leur mot de passe administrateur volés, soit ont subi des attaques massive par déni de service distribué. Ces sites comprennent des blogs personnels (Osin, Vang Anh) et forums de discussion (x-Cafe, Dan Luan, Talawas, DCVOnline), très populaires parmi les lecteurs au Vietnam.

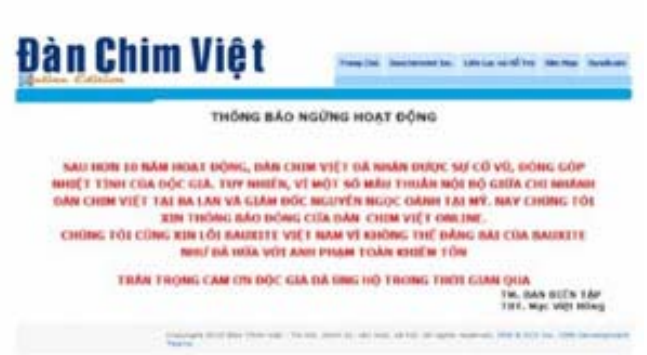


➢Des pirates ont annoncé la fermeture du Blog Osin.

Le journaliste Huy Duc, qui exploite le blog Osin, avait été pris pour cible par les autorités pendant plus d'un an. Sous la pression du gouvernement, son employeur, un journal lié à l'Etat, a été contraint de le licencier en juin 2009 après que Huy Duc ait écrit un article sur son blog à propos de l'inhumanité du mur de Berlin. Lorsque les pirates ont pris le contrôle de son site en janvier 2010, ils ont affiché un faux billet d'adieu d'Osin aux lecteurs. L'annonce humiliante disait qu'Osin fermait son blog parce qu'il « manquait d'inspiration » et devait s'occuper de « son épanouissement personnel, et subvenir à ses besoins en nourriture et en vêtements. »

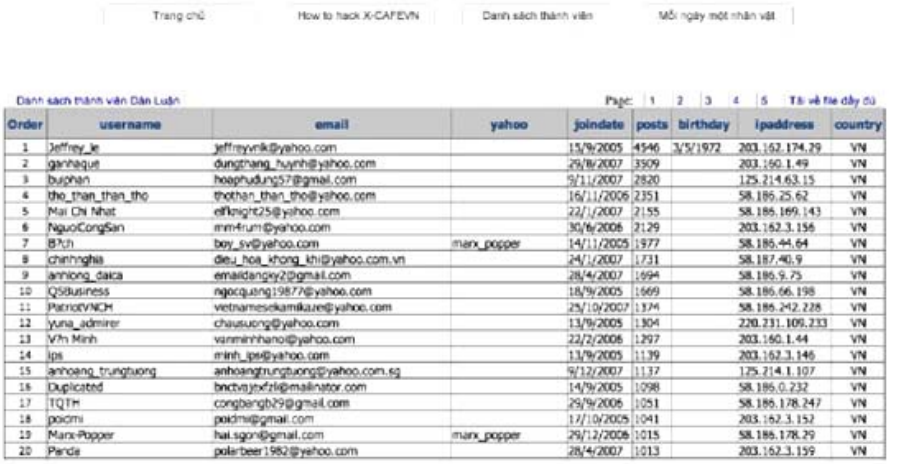
Le journaliste Huy Duc, qui exploite le blog Osin, avait été pris pour cible par les autorités pendant plus d'un an. Sous la pression du gouvernement, son employeur, un journal lié à l'Etat, a été contraint de le licencier en juin 2009 après que Huy Duc ait écrit un article sur son blog à propos de l'inhumanité du mur de Berlin. Lorsque les pirates ont pris le contrôle de son site en janvier 2010, ils ont affiché un faux billet d'adieu d'Osin aux lecteurs. L'annonce humiliante disait qu'Osin fermait son blog parce qu'il « manquait d'inspiration » et devait s'occuper de « son épanouissement personnel, et subvenir à ses besoins en nourriture et en vêtements. »

Une note fictive est également apparue sur DCVOnline.net après que le site d'information et de discussion ait été piraté. La note annonçait la fermeture du site en raison de conflits internes et présentait ses excuses aux lecteurs pour ne pas avoir publié un article prétendument envoyé par l'un des organisateurs de Bauxite Vietnam.



➢Des pirates ont laissé un message sur DCVOnline.net

Dans une volonté visant à intimider la communauté des internautes vietnamiens, à l'intérieur du pays comme à l'étranger, les pirates ont mis en ligne les données personnelles des membres du forum de discussion x-cafevn.org, après avoir piraté le site en question. Les noms d'utilisateur, les adresses email, les lieux de résidence et les adresses IP de plus de 19.000 utilisateurs ont été affichés publiquement. En outre, les profils des présumés administrateurs et des divers militants des droits de l'homme associés à x-cafevn.org ont également été affichés sur www.x-cafevn-db.info.



Order	username	email	yahoo	joindate	posts	birthday	ipaddress	country
1	Jeffrey_le	jeffreyvnk@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	bugnhan	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	NguoCongSan	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	anniong_daica	emaildangky2@gmail.com		28/4/2007	1694		58.186.9.75	VN
10	QSdusiness	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	Vh 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	anhoangtrungtuong	anhoangtrungtuong@yahoo.com.sg		9/12/2007	1137		125.214.1.107	VN
16	Duplicated	bncbvjpxfzl@mailinator.com		14/9/2005	1098		58.186.0.232	VN
17	TQTH	congbangth29@gmail.com		29/9/2006	1051		58.186.178.247	VN
18	paomi	paolms@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	polarbear1982@yahoo.com		28/4/2007	1013		203.162.3.159	VN

➢Des informations privées des membres du forum X-café ont été mis en ligne par les pirates.

Selon des personnes bien informées de la situation, ces profils mélangent habilement vraies et fausses informations. L'objectif est de faire croire aux internautes que des agents de renseignement de Hanoi travaillent avec les pirates et peuvent obtenir des dossiers sur pratiquement n'importe quel militant vietnamien ou utilisateur d'internet. Les pirates ont eu accès à x-cafevn.org à l'aide de logiciels malveillants leur permettant de voler le mot de passe d'un des administrateurs du site.

LES CYBER-ATTAQUES CONTRE VIET TAN

Le site internet de Viet Tan fait régulièrement l'objet d'attaques de type DoS (déni de service) et DdoS (déni de service distribué) de niveaux faible à modéré.

Le 30 avril 2009, viettan.org était victime d'une attaque majeure de déni de service. Nous pensons que, depuis le Vietnam, les pirates ont employé la méthode d'attaque de type xFlash. Ils ont piraté plusieurs autres sites et installé un programme nommé vnattackerpop.swf. Les visiteurs de ces sites déclenchent sans le vouloir sur leurs ordinateurs l'exécution d'un script qui consiste à envoyer une requête au site viettan.org. Sur une période de cinq jours, le serveur viettan.org a été inondé de dizaines de millions de demandes.

Viet Tan a contacté les sites contenant le script d'attaque et leur a demandé de faire le ménage. Peu de temps après, les attaques par déni de service ont cessé. Le moment de l'attaque avait une signification politique. En effet, le 30 avril marque la chute de Saigon, tombée aux forces communistes.

Le serveur de viettan.org a également connu de nombreuses tentatives d'intrusion non autorisée. Les comptes de la messagerie interne ont fait l'objet de tentatives de craquage de mot de passe par force brute. Ces attaques se déroulent régulièrement. Lorsque nous bloquions les adresses IP utilisées pour ces tentatives, les pirates se servaient d'une autre série d'adresses IP.

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

➢Liste partielle des cyber-attaques contre des sites basés à l'étranger.

Le site viettan.org est généralement bloqué par un pare-feu au Vietnam. Mais parfois, les utilisateurs d'Internet au Vietnam ont signalé que ce pare-feu était levé et qu'ils pouvaient accéder au site web de Viet Tan. Cette ouverture du pare-feu coïncide généralement avec une attaque de type déni de service en provenance du Vietnam - preuve que les cyber-attaques sont lancées avec le consentement, si ce n'est avec l'ordre, des autorités vietnamiennes.

Outre le ciblage des serveurs informatiques de Viet Tan, les pirates ciblent délibérément des membres de Viet Tan en leur envoyant des courriels contenant des logiciels malveillants sous couvert de documents normaux. Quelques membres de Viet Tan ont vu leurs ordinateurs infectés par ces logiciels malveillants permettant aux pirates d'obtenir les mots de passe des comptes de messagerie. Récemment, les pirates ont publié ces informations sur www.x-cafevn-db.info, pour vanter leurs exploits.

RECOMMANDATIONS

1. Condamner les cyber-attaques des autorités vietnamiennes

En ciblant les sites web et les internautes à l'extérieur du Vietnam, le gouvernement de Hanoi ne veut plus seulement limiter la liberté d'expression aux citoyens vietnamiens. Il veut également s'en prendre aux droits et à la vie privée des internautes à travers le monde. Les cyber-attaques et le vol de données utilisateurs constituent une violation des lois nationales. Les administrations au Vietnam qui sont derrière ces activités illégales doivent rendre des comptes devant les instances judiciaires.

2. Demander au gouvernement vietnamien de respecter la liberté d'Internet

Le gouvernement vietnamien doit abroger les lois qui pénalisent l'expression pacifique. En particulier, le décret n° 97/2008/ND-CP sur la gestion des blogs et la directive du Ministère de la Sécurité Publique pour bloquer Facebook sont incompatibles avec les conventions internationales des droits de l'homme auxquelles le Vietnam est signataire. La censure d'Internet est également contraire à l'objectif soutenu par le gouvernement vietnamien de développer une économie fondée sur le savoir.

3. Demander au gouvernement vietnamien de libérer les blogueurs et cyber-militants emprisonnés

Vous pouvez attirer l'attention du public sur les cas des blogueurs et des militants vietnamiens qui sont emprisonnés pour l'expression pacifique de leurs opinions. Exprimez votre solidarité avec ces prisonniers de conscience et offrez un soutien à leurs familles.

4. Promouvoir la connaissance de la sécurité sur Internet et des méthodes de contournement des pare-feu

Vous pouvez également aider les internautes vietnamiens à contourner les pare-feu du gouvernement et les protéger contre le piratage à travers une assistance technique, financière et éducative. Cette connaissance peut aider les blogueurs vietnamiens à être plus efficaces dans leur travail de journalisme citoyen, de défense des droits de l'homme et de construction de la société civile.

À PROPOS DE VIET TAN

La mission de Viet Tan est de mettre fin à la dictature, construire les fondements pour une démocratie durable, demander la justice et les droits de l'homme pour le peuple vietnamien à travers une lutte non violente, basée sur la participation civile.

Comment s'impliquer ?

Soutenez les campagnes en cours de Viet Tan et faites-nous savoir si vous souhaitez participer à la prochaine activité de Viet Tan dans votre région.

Visitez notre site internet, rejoignez notre liste de diffusion et aidez-nous à diffuser des informations sur nos activités et la situation au Vietnam. Vous pouvez également nous retrouver sur Twitter et Facebook.

Nous accueillons les nouveaux membres et les partisans qui veulent contribuer aux changements qu'ils souhaitent pour le Vietnam.