secdev.foundation

7 September 2016 Volume # 15

FLASH NOTES

"Short analytical briefs on emerging topics related to The SecDev Foundation's work"

VIETNAMESE CYBER SECURITY LAW THREATENS PRIVACY RIGHTS AND ENCRYPTION

Vietnam's government just opened a backdoor into encrypted communications. Vietnamese social activists should take note.

Vietnam is among the world's most targeted countries given its ongoing diplomatic tensions with China.[1] The July cyber attack on Noi Bai Airport underlined the scale of Vietnam's cyber crime and hacking woes. Malware delivered to unsuspecting internet users, including staff of government agencies, is seen as a main entry point for hackers.

It is timely, then, that on 1 July Vietnam enacted the 2015 Cyber Information Security Law. The law sets out a system to classify digital information and specify the steps public organizations need to follow to protect such data. It mandates the Ministry of Communication and Information (MCI) and the Vietnam Computer Emergency Response Team (VNCERT) as the leaders in the nation's battle against cyber crime.

TIA SANG VIETNAM

Tia Sáng Viêt Nam supports online safety and internet freedom in Vietnam. The initiative aims to support a range of stakeholders by researching internet and society issues and making strategic interventions to support online safety and cyber security among Vietnamese youth.

1. Network security firm Crowdstrike in its 2014 Global Threat Report: "Vietnam and (Chinese malware group) Goblin Panda were respectively the most targeted country and the most active adversary."

A Facebook user posts a photo of a handwritten boarding pass, as all airport systems went down as a result of the hack.

The law, on its surface, includes protections for individuals' privacy and unhindered use of the internet. Scratch deeper, however, and it is clear that user rights are secondary to any perceived national security and 'social order' concerns. In particular, the law can be used to restrict the use of encrypted communications by private citizens, and seize and decrypt data in seemingly any case deemed necessary.

First, the Good News

The law, in principle, protects the right to privacy of information. The response to cyber information security incidents "may not infringe upon privacy, personal and family secrets of individuals and private information of organizations."

The law also stipulates that no one can block or filter the internet, as prohibited acts include "blocking the transmission of information in cyberspace" and "illegally affecting or obstructing the normal operation of information systems or the users' accessibility to information systems."

The law also considers encryption: "Hacking cryptographic secrets and lawfully enciphered information of agencies, organizations or individuals" is prohibited – although this article also notes that "using or trading in civil cryptographic products of unclear origin" is also prohibited (as commercial encryption tools and services will often need to be licensed, see below).

But in the End, Security Triumphs

In Section 2, Article 16 of the Cyber Information Security Law, personal privacy is made subservient to other laws on security and defense:

> ***"The processing of personal information for the purpose of ensuring national defense and security and social order and safety or for non-commercial purposes must comply with other relevant laws."***

The third chapter of the law deals with 'civil cryptography' (the storing, sending and receiving of encrypted messages). From a rights perspective, this chapter and the subsequent July 2016 Decree on Civil Cryptography is greatly concerning.[2]

Encryption tools and services are now divided into two overarching categories – those that require a license and those that can be freely distributed without a license.

Widely used free chat services like WhatsApp, which employ end-to-end encryption, should not require a license: "Operating systems, Internet browsers and software with integrated cryptographic components (though cryptographic protection of information is not the primary function), which are used on a grand scale and developed to be installed by users without providers' help" are exempted.

However, all other tools and services focused on encryption, presumably including PGP email (an open source tool) and other services using a PKI (public key infrastructure) system, now require a lengthy and complex licensing process (with operations in Vietnam) in order to be legally used in Vietnam.3

In addition to paying a licensing fee, enterprises that wish to trade in civil cryptographic products and services must be found technically competent, have a business plan conforming to regulations, and a cyber-information, confidentiality and security plan in place.

Beyond the bureaucratic difficulties of the licensing process, the law also stipulates the need for a backdoor into encrypted information.

Article 36 states that the responsibilities of users of cryptographic products and services include: "To provide necessary information relating to cryptographic keys for competent state agencies upon request." Furthermore, all users other than diplomatic missions and intergovernmental agencies will need to declare their use of civil cryptographic products to the Government Cipher Committee.

The July 2016 Decree on Civil Cryptography takes this troubling language further, with vague wording that ultimately empowers the government to access encrypted information (see points c and d, below), with a fine imposed on any person or organization that does not cooperate:

Decree 58/2016

Article 7:

3. A fine of VND 40,000,000 to VND 50,000,000 shall be imposed against:

a. Sale of civil cryptography products and services, exportation or importation of civil cryptography products without a license...;

b. Failure to cease or terminate the provision of civil cryptography products and services for purposes of national defense, national security, social order or safety upon requests by competent governmental authorities;

c. Failure to cooperate or support competent governmental authorities' performing professional measures upon requests;

d. Refusal to provide essential information on cryptographic keys upon requests by competent governmental authorities.

An overseas Vietnamese lawyer, who asks not to be named, finds fault with these points: "Failure to comply with the 'requests' or refusal to provide information on cryptographic keys carry the heaviest of penalties in the Decree. Furthermore, these requests do not require any court involvement or any specific process. For that matter, there's no mention of the principle of personal privacy."

Vietnam's social activists have been largely silent on the 2015 Cyber Information Security Law and the subsequent Decree on Civil Cryptography. It is a technical area that is not widely understood or reported on.

There is no data available on the use of encrypted communications in Vietnam, but anecdotal reports among activist circles indicate

2. Full name: Decree 58/2016/ND-CP on the Sale and Provision of Civil Cryptography Products and Services and the Exportation or Importation of Civil Cryptography Products.

3. Whether chat tools that specifically market their secure, encrypted capabilities (Signal, Telegram, ChatSecure) will be exempt from licensing is not clear.

it is rarely used. Among mainstream internet users, WhatsApp is not popular compared to domestic chat tool Zalo and Facebook Messenger (both unencrypted).

As Vietnam's citizens become ever more internet savvy and active, interest in encryption is likely to grown. It is particularly relevant given Vietnam's high cyber crime environment. This new decree, if passed, will likely help to stifle the evolution to more secure communications. It will be interesting to see how Vietnam's government balances the cost of monitoring and controlling civilian use of encryption versus the need for privacy and data protection in preventing cyber crime and widespread network attacks.

The Noi Bai Airport hack saw arrival-departure screen displays replaced with this image warning Vietnam and The Philippines to stay out of China's sovereign territory.

WRITTEN BY : MICHAEL L. GRAY

THE SECDEV FOUNDATION

The SecDev Foundation is an Ottawa-based think-do tank that works at the cross-roads of security, development and new technology. The SecDev Foundation believes that information can change the world. We see that new technologies can empower people out of conflict, insecurity and oppression. Our mission is to understand how; our goal is to help that change happen.