PwC in the News

Sep 2016

Media title: Coordinated Defense
Author: Robert Trong Tran, Director of Cyber Security Services, PwC Vietnam
Source: Vietnam Economic Times dated 15 Sep 2016

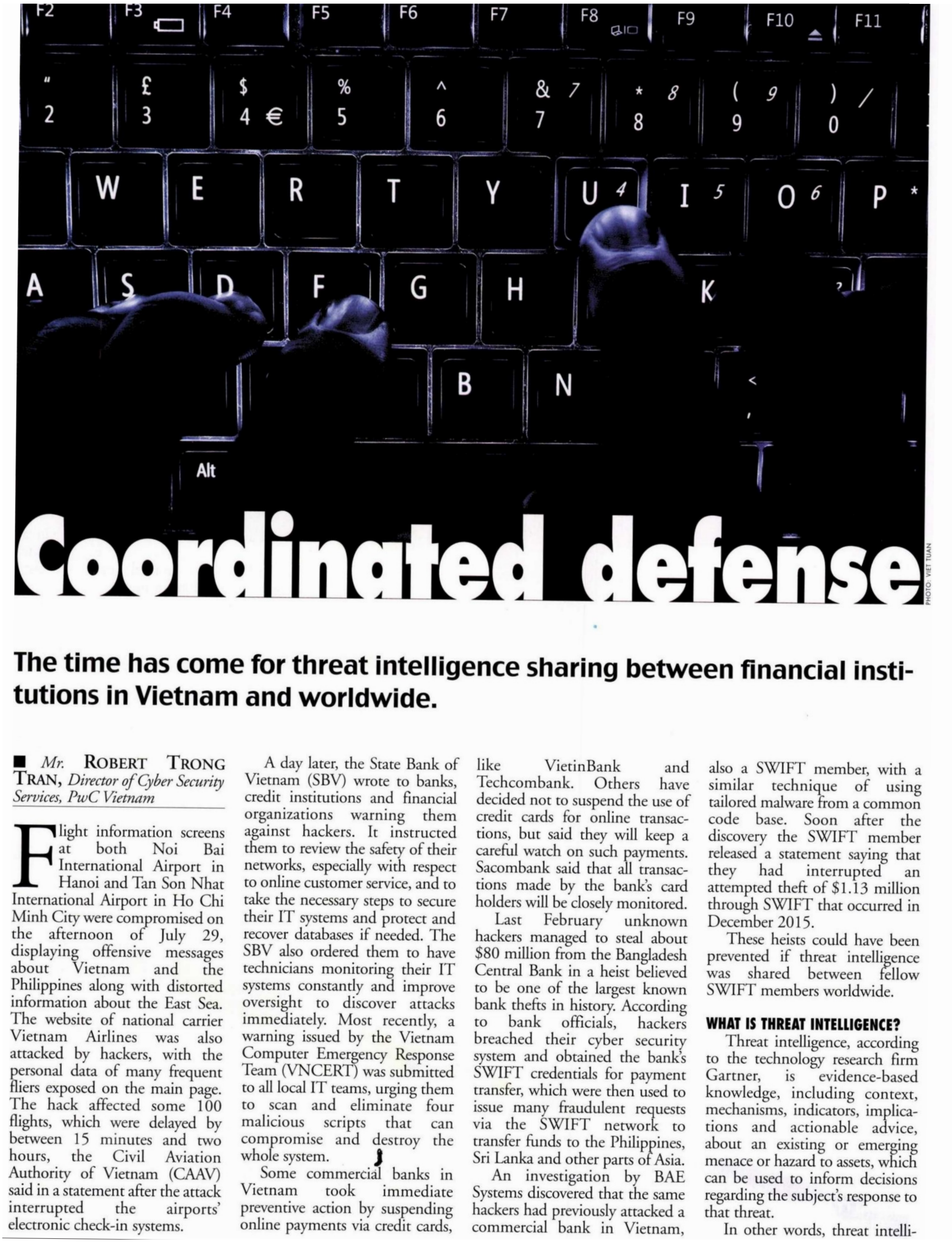


PHOTO: VIET TUAN

Coordinated defense

The time has come for threat intelligence sharing between financial institutions in Vietnam and worldwide.

■ *Mr.* ROBERT TRONG TRAN, *Director of Cyber Security Services, PwC Vietnam*

Flight information screens at both Noi Bai International Airport in Hanoi and Tan Son Nhat International Airport in Ho Chi Minh City were compromised on the afternoon of July 29, displaying offensive messages about Vietnam and the Philippines along with distorted information about the East Sea. The website of national carrier Vietnam Airlines was also attacked by hackers, with the personal data of many frequent fliers exposed on the main page. The hack affected some 100 flights, which were delayed by between 15 minutes and two hours, the Civil Aviation Authority of Vietnam (CAAV) said in a statement after the attack interrupted the airports' electronic check-in systems.

A day later, the State Bank of Vietnam (SBV) wrote to banks, credit institutions and financial organizations warning them against hackers. It instructed them to review the safety of their networks, especially with respect to online customer service, and to take the necessary steps to secure their IT systems and protect and recover databases if needed. The SBV also ordered them to have technicians monitoring their IT systems constantly and improve oversight to discover attacks immediately. Most recently, a warning issued by the Vietnam Computer Emergency Response Team (VNCERT) was submitted to all local IT teams, urging them to scan and eliminate four malicious scripts that can compromise and destroy the whole system.

Some commercial banks in Vietnam took immediate preventive action by suspending online payments via credit cards, like VietinBank and Techcombank. Others have decided not to suspend the use of credit cards for online transactions, but said they will keep a careful watch on such payments. Sacombank said that all transactions made by the bank's card holders will be closely monitored.

Last February unknown hackers managed to steal about $80 million from the Bangladesh Central Bank in a heist believed to be one of the largest known bank thefts in history. According to bank officials, hackers breached their cyber security system and obtained the bank's SWIFT credentials for payment transfer, which were then used to issue many fraudulent requests via the SWIFT network to transfer funds to the Philippines, Sri Lanka and other parts of Asia.

An investigation by BAE Systems discovered that the same hackers had previously attacked a commercial bank in Vietnam, also a SWIFT member, with a similar technique of using tailored malware from a common code base. Soon after the discovery the SWIFT member released a statement saying that they had interrupted an attempted theft of $1.13 million through SWIFT that occurred in December 2015.

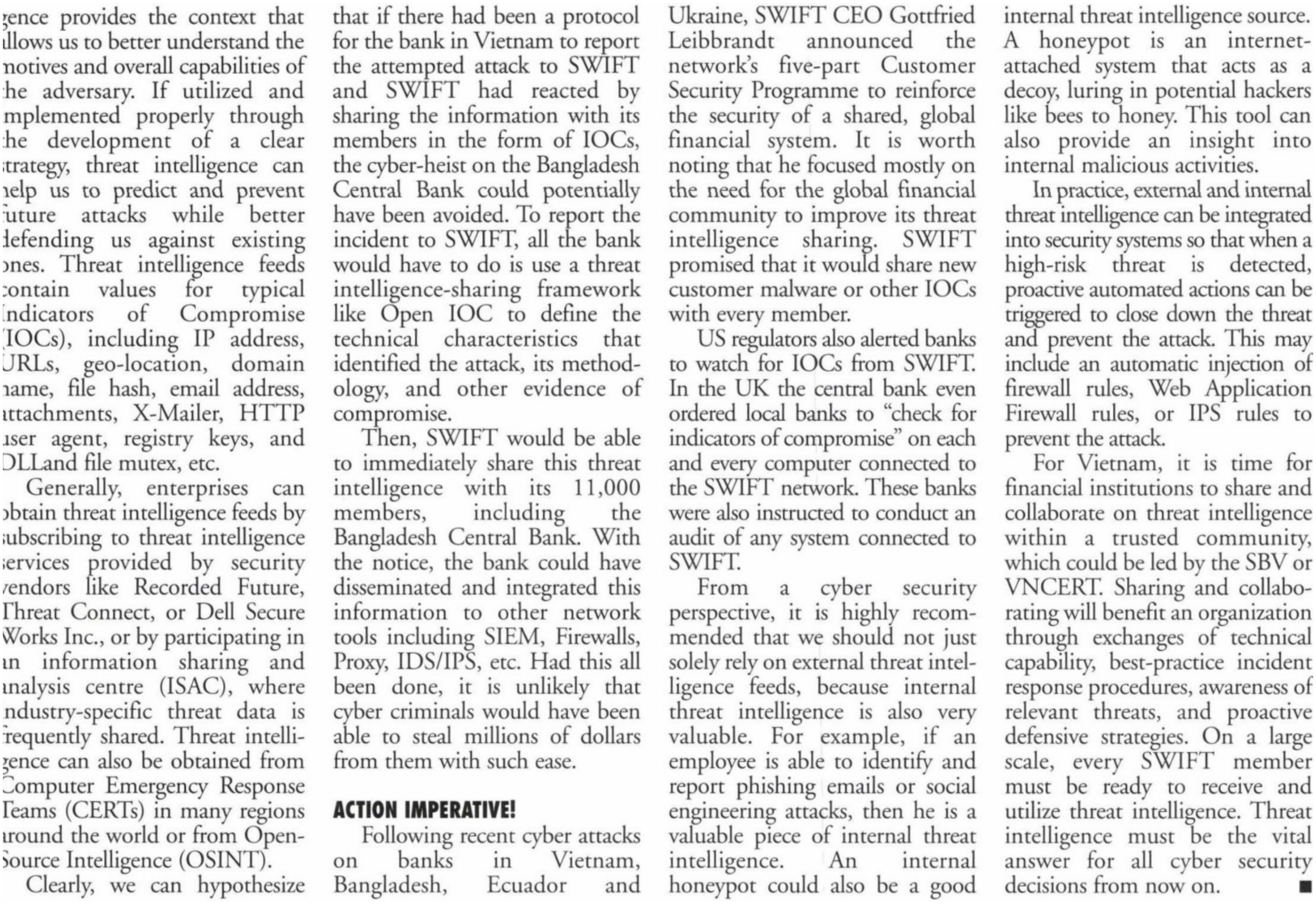
These heists could have been prevented if threat intelligence was shared between fellow SWIFT members worldwide.

WHAT IS THREAT INTELLIGENCE?

Threat intelligence, according to the technology research firm Gartner, is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets, which can be used to inform decisions regarding the subject's response to that threat.

In other words, threat intelli-

Media title: Coordinated Defense
Author: Robert Trong Tran, Director of Cyber Security Services, PwC Vietnam
Source: Vietnam Economic Times dated 15 Sep 2016



gence provides the context that allows us to better understand the motives and overall capabilities of the adversary. If utilized and implemented properly through the development of a clear strategy, threat intelligence can help us to predict and prevent future attacks while better defending us against existing ones. Threat intelligence feeds contain values for typical Indicators of Compromise (IOCs), including IP address, URLs, geo-location, domain name, file hash, email address, attachments, X-Mailer, HTTP user agent, registry keys, and DLLand file mutex, etc.

Generally, enterprises can obtain threat intelligence feeds by subscribing to threat intelligence services provided by security vendors like Recorded Future, Threat Connect, or Dell Secure Works Inc., or by participating in an information sharing and analysis centre (ISAC), where industry-specific threat data is frequently shared. Threat intelligence can also be obtained from Computer Emergency Response Teams (CERTs) in many regions around the world or from Open-Source Intelligence (OSINT).

Clearly, we can hypothesize that if there had been a protocol for the bank in Vietnam to report the attempted attack to SWIFT and SWIFT had reacted by sharing the information with its members in the form of IOCs, the cyber-heist on the Bangladesh Central Bank could potentially have been avoided. To report the incident to SWIFT, all the bank would have to do is use a threat intelligence-sharing framework like Open IOC to define the technical characteristics that identified the attack, its methodology, and other evidence of compromise.

Then, SWIFT would be able to immediately share this threat intelligence with its 11,000 members, including the Bangladesh Central Bank. With the notice, the bank could have disseminated and integrated this information to other network tools including SIEM, Firewalls, Proxy, IDS/IPS, etc. Had this all been done, it is unlikely that cyber criminals would have been able to steal millions of dollars from them with such ease.

ACTION IMPERATIVE!

Following recent cyber attacks on banks in Vietnam, Bangladesh, Ecuador and Ukraine, SWIFT CEO Gottfried Leibbrandt announced the network's five-part Customer Security Programme to reinforce the security of a shared, global financial system. It is worth noting that he focused mostly on the need for the global financial community to improve its threat intelligence sharing. SWIFT promised that it would share new customer malware or other IOCs with every member.

US regulators also alerted banks to watch for IOCs from SWIFT. In the UK the central bank even ordered local banks to "check for indicators of compromise" on each and every computer connected to the SWIFT network. These banks were also instructed to conduct an audit of any system connected to SWIFT.

From a cyber security perspective, it is highly recommended that we should not just solely rely on external threat intelligence feeds, because internal threat intelligence is also very valuable. For example, if an employee is able to identify and report phishing emails or social engineering attacks, then he is a valuable piece of internal threat intelligence. An internal honeypot could also be a good internal threat intelligence source. A honeypot is an internet-attached system that acts as a decoy, luring in potential hackers like bees to honey. This tool can also provide an insight into internal malicious activities.

In practice, external and internal threat intelligence can be integrated into security systems so that when a high-risk threat is detected, proactive automated actions can be triggered to close down the threat and prevent the attack. This may include an automatic injection of firewall rules, Web Application Firewall rules, or IPS rules to prevent the attack.

For Vietnam, it is time for financial institutions to share and collaborate on threat intelligence within a trusted community, which could be led by the SBV or VNCERT. Sharing and collaborating will benefit an organization through exchanges of technical capability, best-practice incident response procedures, awareness of relevant threats, and proactive defensive strategies. On a large scale, every SWIFT member must be ready to receive and utilize threat intelligence. Threat intelligence must be the vital answer for all cyber security decisions from now on. ■