SWIFT:
RISKS OF FINANCIAL SYSTEM IN A CYBER ERA

Giacomo Minello

March 2020

Assignment

1. How were the various banks attacked? Why was the attack on CBB successful? Was it different in the case of other banks?
2. How did the series of attacks impact on the banks involved and on the SWIFT system?
3. What type of solutions you could envisage to guarantee the correct working of this critical infrastructure of global financial markets?

Contents

1 The attacks **1**

1.1 SWIFT 1

1.2 Timeline of high-profile SWIFT-related attacks 7

1.2.1 Sonali Bank, Bangladesh - 2013 7

1.2.2 Banco del Austro, Ecuador - January, 2015 8

1.2.3 Tien Phong Bank, Vietnam - December, 2015 9

1.2.4 The Bank of Bangladesh, Bangladesh - February, 2016 12

1.2.5 Unnamed Ukrainan bank - 2016 17

1.2.6 Polish Financial Supervision Authority (Komisja Nadzoru Finansowego) - January, 2017 17

1.2.7 Russian bank - 2017 19

1.2.8 The Far Eastern International, Taiwan - October, 2017 20

1.2.9 NIC Asia Bank, Nepal - October, 2017 20

1.2.10 City Union Bank, India - February, 2018 21

1.2.11 Banco de Chile - May, 2018 22

1.2.12 Cosmos Bank, India - August, 2018 23

1.3 The attackers - APT38 a.k.a. Lazarus Group 24

2 The consequences **31**

2.1 The aftermath 31

2.2 The investigation 32

2.3 Customer Security Programme and Information Sharing and Analysis Centre 36

3 The solutions **41**

3.1 CSP and complementary solutions 41

3.1.1 Predict 44

3.1.2 Prevent 44
3.1.3 Detect 44
3.1.4 Respond 45

References **46**

List of Figures

1 V-shaped message flow structure. 4
2 Y-copy message flow via SWIFTNet. 5
3 Local SWIFT infrastructure model 6
4 Timeline of the attacks 7
5 Sonali Bank Hack 8
6 Banco del Austro Hack 9
7 Tien Phong Bank Hack 10
8 Timeline of the Tien Phong Bank attack according to Kaspersky Lab. 11
9 Bank of Bangladesh Hack 15
10 How the malware exploited liboradb.dll 16
11 http://www.knf.gov.pl 18
12 Far Eastern International Bank Hack 20
13 APT38/Bluenoroff tactics, techniques an procedures 25
14 Swift Hacks 26
15 North Korean intelligence structure 29
16 Park Jin Hyok most wanted poster 35
17 SWIFT CSP Security controls implementation timeline 37
18 SWIFT CSP Framework Objectives and Principles 38
19 SWIFT counterparty cybersecurity risk 38
20 Extract of the mapping between SWIFT security controls and other industry standard 41
21 Attack Vectors due to weak security 42
22 Attack Vector after implementing SWIFT CSP 43

List of Tables

1 Description of payment system processes. 3

1 The attacks

1.1 SWIFT

SWIFT (the Society for Worldwide Interbank Financial Telecommunications) is a secure messaging service used to transmit financial messages between member institutions around the world.

SWIFT has served the financial services sector as proprietary communications platform, provider of products and services, standards developer, and conference organizer (Sibos). Founded to create efficiencies by replacing telegram and telex (or "wires") for international payments, SWIFT now forms a core part of the financial services infrastructure.

SWIFT functions as a member-only cooperative service that is used and trusted by more than 11,000 financial institutions in more than 200 countries and territories around the world.

It is important to clarify that SWIFT is not a payment system but serves as a transport network for a large number of major payment and securities infrastructures. This makes it the most significant provider of global financial messaging and processing services in the world today, a position that its cooperative status is designed to mitigate. The majority of financial institutions use SWIFT to send and receive information about financial transactions. However, SWIFT does not maintain financial information on an ongoing basis and data are only held for a limited period of time. Rather, SWIFT is responsible for providing the network, standards, products, and services that allow member institutions to connect and exchange financial information.

SWIFT distinguishes itself from public Internet Protocol networks by accepting limited liability for defined categories of loss resulting from transaction message delays that have arisen as a consequence of technical issues within SWIFT. Financial service professionals say that the most critical part of SWIFT's role is achieving the secure exchange of proprietary data – in other words: reliability, confidentiality, and integrity

Although sometimes referred to as not for profit, SWIFT is more accurately

committed to being a "not-for-profit maximization" organization. Over the last ten years, SWIFT management have prioritized a reduction in per message costs. The cooperative status also imposes certain obligations on members to support SWIFT in kind, through contribution of relevant expertise and an undertaking to route a substantial portion of messaging through SWIFT. However, not all organizations that use the SWIFT network are eligible to be shareholders. SWIFT users are grouped into three categories, each of which has access to different levels of service from SWIFT: supervised financial institutions can send and receive all types of messages; non-supervised entities active in the financial industry can send all type of messages to supervised financial institutions but cannot send or receive payment messages to or from other non-supervised entities; and closed user groups and corporate entities have access to services as defined by the administrator of the closed user group or, for corporate entities, according to criteria defined in the relevant service. Only members of the first category – who are banks, securities broker-dealers, and regulated investment management institutions – would be eligible to be shareholders of SWIFT.

Management of SWIFT is organized among three groups (marketing, IT operations, and finance and administration) and two functions (legal and human resources), across three regions (Americas, Asia-Pacific, and EMEA). Marketing has a broad brief encompassing product portfolio management, global communication, innovation, and standards. IT operations is not only responsible for the day-to-day running of the SWIFT network but also product development and security control. Finance and administration is responsible for financial management, corporate planning, and pricing of products as well as all internal support functions such as procurement, internal IT, and office management. Payments between counterparties are not generally processed instantly, which means that payment systems will often process payments and monetary claims on the basis of "promises to pay", rather than actual transfer of funds. To facilitate this exchange and guarantee as much as possible the completion of the transaction, payment systems initiate a sequence of events that involves a number of financial institutions and technologies such as banks, clearinghouses, data transmission links, and electronic accounting systems. There are generally three basic stages or processes which are triggered each time a payment needs to be executed, as we can see in table 1.

Table 1: Description of payment system processes.

Payment stage	*Description*
1. Authorization and initiation of the payment	This stage involves the submission of the payment order by the payer in order for the funds to be transferred.
2. Transmission and exchange of the payment instructions	This involves the transmission and exchange of obligations between the parties involved in the transaction. This process may also include the netting (or offsetting) of the obligations where necessary.
3. Settlement of the payment	This final stage entails the compensation sent from the payer's bank to the payee's bank. A third-party settlement agent is usually involved in this process.

At each step of the payment lifecycle, the payment system must be efficient and reliable in order to avoid any operational and financial risks and ultimately ensure the exchange of funds. Such time-sensitive systems, often referred to as Large-Value Payment Systems (LVPS), usually incorporate real-time gross settlement (RTGS) as part of their payment process. Since the attributes of such systems, and the risks associated, are of great interest to central banks, it is common that they will be actively involved in the governance and decision-making that control these. Quite often central banks will own the domestic LVPSs and operate the various payment and settlement services, though when this is not the case they will monitor operations and oversee any developments while ensuring that the payment systems generally comply with the core principles identified by regulations. Typically, when central banks do not own the system themselves they act as settlement agents within the payment process.

In the case of cross-border payments, depending on the payment system architecture, the routing of the messages (the second stage of the payment) can take many different forms. The simplest and most popular structure of message flows used by the majority of RTGS systems around the world is

the V-shaped structure depicted in figure 1.

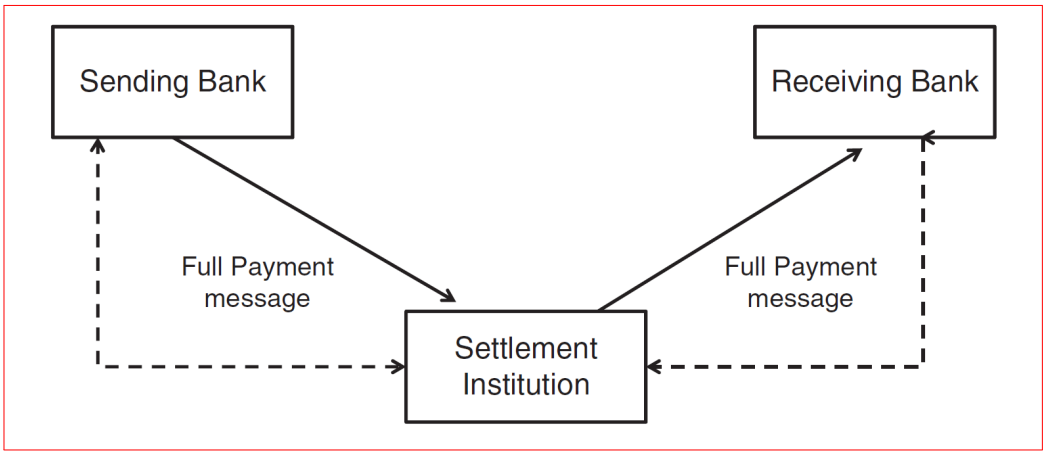

Figure 1: V-shaped message flow structure.

SWIFT has designed and operates the Y-copy routing, a sophisticated message flow arrangement where SWIFT intercepts the message, copies the entire content of the message, and sends this copy to the settlement institution. Once the SWIFT network receives a respective approval and settlement message from the settlement institution, it forwards the original payment message to the receiving institution as summarized in figure 2.

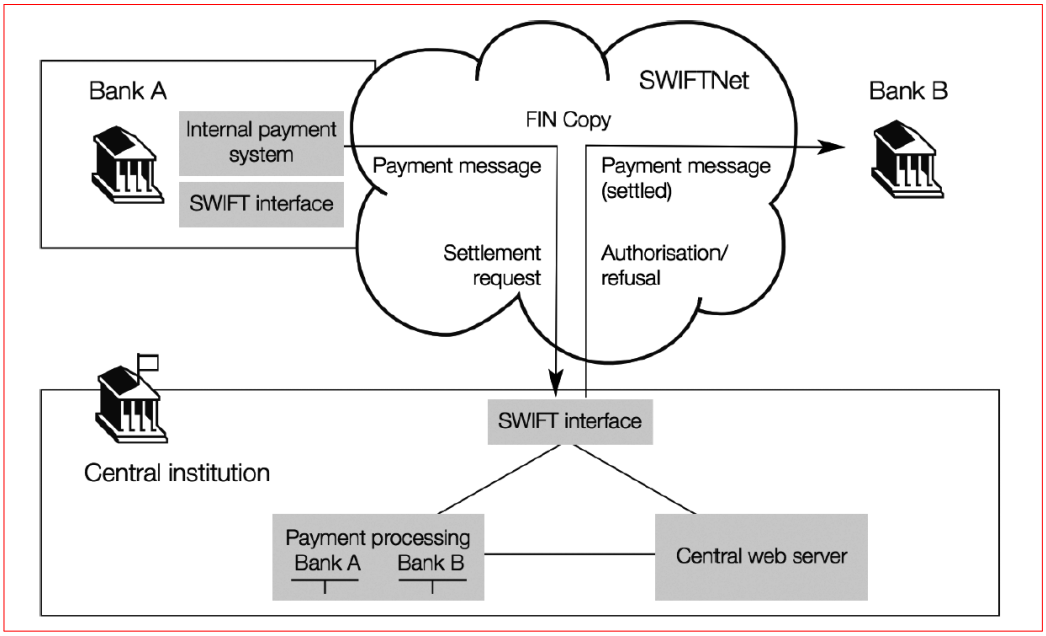

Figure 2: Y-copy message flow via SWIFTNet.

SWIFT complements the process with a number of query and reporting features that provide users with information useful for their payment operations (e.g. better liquidity management and to achieve reconciliation in case of system outages). Ensuring the integrity of the message is one of the key roles of SWIFT.[1]

SWIFT does not, however, hold responsibility for the security of its customers' local SWIFT infrastructure, although it does provide assistance to ensure customers are able to manage cyber attacks. An example of this is the Customer Security Programme (CSP), which was originally introduced in late 2016. A diagram representing how Full Stack local SWIFT infrastructure model should be secured can be seen in figure 3.

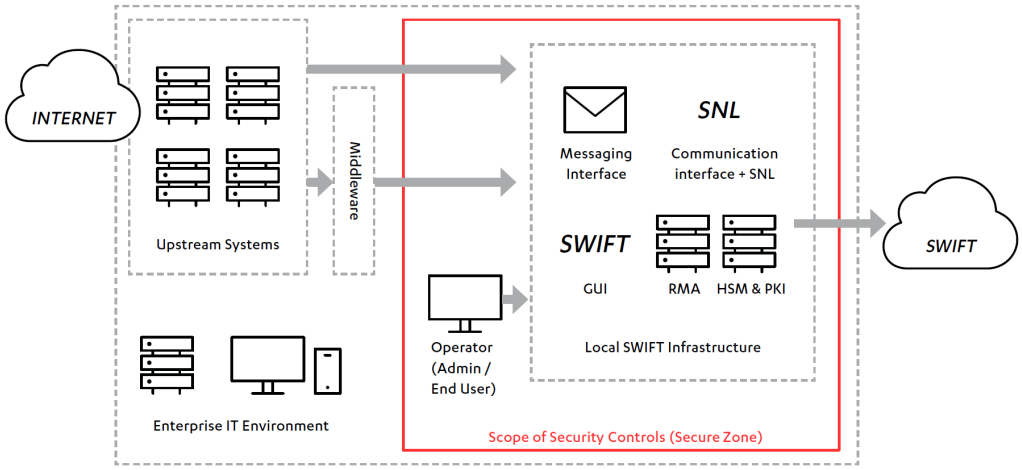

Figure 3: Local SWIFT infrastructure model

The components shown in figure 3 are broken down as follows:

- Secure Zone - a segmented portion of the network, isolating SWIFT systems from the rest of the enterprise environment.
- Messaging Interface - a software product (e.g. Alliance Access) supporting the use of SWIFT's messaging services. This is typically connected directly to the Communication Interface.
- Communication Interface - a software product (e.g. Alliance Gateway) that provides a link between the SWIFT network (SWIFTNet) and the Messaging Interface software.
- SWIFTNet Link (SNL) - a mandatory software product for access to messaging services over a secure IP network (within the above diagram the SNL is part of the Communication Interface).
- HSM & PKI - the SWIFT Hardware Security Module and Public Key Infrastructure.
- RMA - the Relationship Management Application (RMA) is a SWIFT-mandated filter that enables customers to define which counterparties are permitted to send FIN messages to the institution.

- Operators - individual end users and administrators who directly interact with the local SWIFT infrastructure trough computer devices used to operate or maintain the local SWIFT infrastructure.

1.2 Timeline of high-profile SWIFT-related attacks

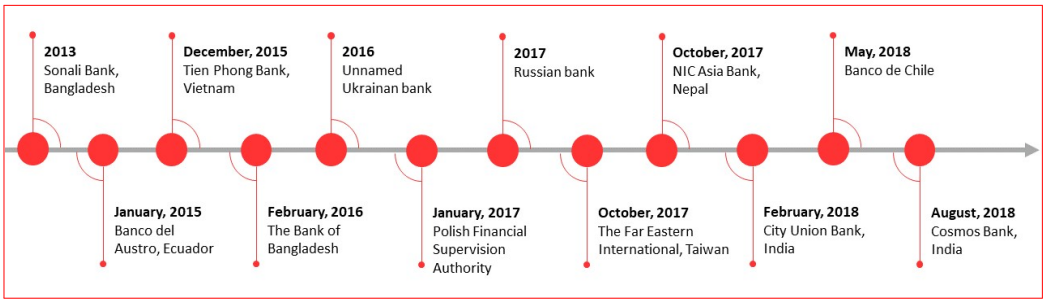

Figure 4: Timeline of the attacks

1.2.1 Sonali Bank, Bangladesh - 2013

Sonali Bank Limited is a state-owned commercial bank in Bangladesh. It is one of the the largest bank of the country.

The unsolved theft of $250,000 at Sonali Bank involved fraudulent transfer requests sent over the SWIFT international payments network. It is not widely known outside of Bangladesh, and until 2016 it was treated as a 'cold case'. However, investigators re-opened the case after the attack on the Bank of Bangladesh.

At Sonali Bank, hackers installed key-logger software on a computer to gain passwords. These credentials were then used to laterally move through the bank's network in order to gain access to the bank's internal SWIFT systems; overall $250,000 worth of SWIFT transactions were made.

Sonali Bank said it had informed SWIFT about the 2013 heist at the time and also unsuccessfully tried to recover the money from the recipients in Turkey.

Police arrested two employees who had responsibility for initiating and approving money transfer instructions, but they were later freed without being

charged.[2]

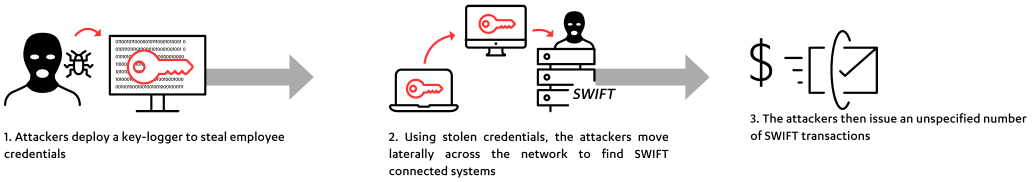

Figure 5: Sonali Bank Hack

1.2.2 Banco del Austro, Ecuador - January, 2015

The attack, occurred on Jan. 21, 2015, resulted in the theft of $12.2 million from Banco del Austro, or BDA, in Ecuador. The theft was revealed via a lawsuit filed by BDA against San Francisco-based Wells Fargo.

The attackers stole the credentials of an unnamed bank employee and used these credentials to access the employee's Outlook email account. Using this access, the attackers located cancelled and rejected SWIFT transfer requests, altered their details, and reissued them.

In this hack, the transfers were made from Banco del Austro HSBC account in San Francisco to HSBC and Hang Seng Bank accounts in Hong Kong, a Wells Fargo account in Los Angeles, a Mashreqbank account in Dubai, and a JPMorgan Chase account in New York. At least $3.1 million of the funds were then routed from those four companies to 19 "second layer" bank accounts, meaning the funds made a second hop to another set of Hong-Kong registered companies. Most of the "second layer" accounts appeared not to be tied to real businesses and to be controlled by citizens of the People's Republic of China, according to Hong Kong Deputy High Court Judge Conrad Seagroatt.

BDA discovered that for each unauthorized transfer, an unauthorized user remotely accessed BDA's computer system after hours, logged onto the SWIFT network purporting to be BDA, and redirected transactions to new beneficiaries with significant dollar amounts.

BDA's lawsuit blame Wells Fargo for failing to spot the fraud. Each of the unauthorized wire transfers were performed outside normal operating hours of Banco del Austro; it included transactions of significant amounts, which should have triggered an alert at Wells Fargo in their control and verification

of the transactions that were being processed.

BDA also discovered that attackers also attempted to transfer another $1.4 million from its Citibank accounts to accounts in Dubai and Hong Kong, but those attacks were blocked. The response of Citibank resulted on the immediate refund of the funds.

Wells Fargo has been blaming BDA's information security policies and procedures for the fraud having occurred and noting that it honored a valid request received via the SWIFT messaging system. For its part, Wells Fargo refunded to BDA $958,700 out of the $1,486,230 it transferred to an account in the name of a Jose Mariano Castillo at Wells Fargo in Los Angeles.[3][4][5][6]

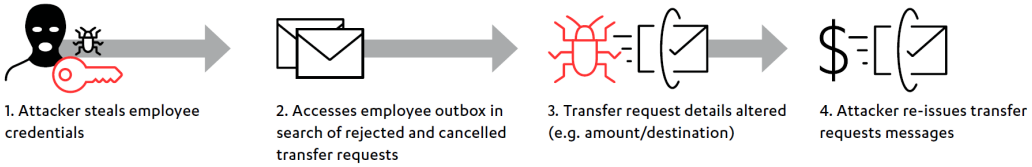

Figure 6: Banco del Austro Hack

1.2.3 Tien Phong Bank, Vietnam - December, 2015

Tien Phong Commercial Joint Stock Bank, based in Hanoi, on May 15 said in a statement to Reuters that it detected suspicious transfer requests for $1.13 million out of its accounts - via the interbank SWIFT messaging system - in the fourth quarter of 2015 as part of a malware attack. The attempted attack did not cause any losses as the bank was quick enough to contact receiving banks and put a stop to the transfers.

The State Bank of Vietnam - the country's central bank – started the investigation on the attack after having received related information from TPBank on May 16.

SWIFT declined to comment on those reports, except to point to a May 13 security alert that it sent to its customers, warning them of "a highly adaptive campaign targeting banks' payment endpoints." That warning said an unnamed Vietnamese bank had been targeted. This led to referring to this attack as an attack towards an "unnamed South-East Asian bank".[7]

TPBank's statement said the fraudulent transfer requests were made using an

unnamed third-party vendor with which the bank had contracted, to allow it to interface with the SWIFT network. The bank said that in the wake of the fraudulent transfer requests, it stopped working with the third-party provider and now has a more secure system which directly interfaces with the SWIFT platform.

It was later discovered that the attack against have been carried out using a Trojanized PDF reader. The malware used to target the bank replaces Foxit's PDF reader software, which was known to be used by the bank employees when viewing SWIFT statements, to mask records of SWIFT transactions when read. When reports are read through the PDF reader, SWIFT records are altered to remove traces of fraudulent transactions.

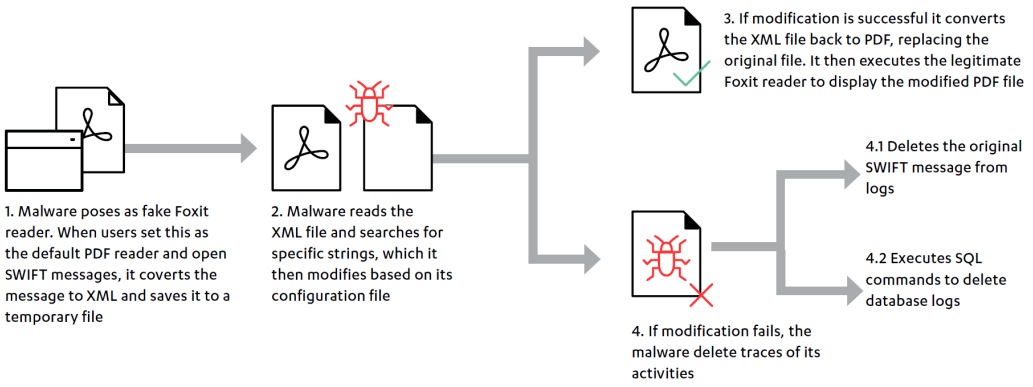

Figure 7: Tien Phong Bank Hack

Attackers were able to install a malicious version of the Foxit PDF reader on employee workstations, which altered statements (when opened) in order to hide evidence of any malicious activity. This malware was found to be installed on infrastructure provided by a third-party vendor, specifically used to provide the bank's connection into the SWIFT messaging network, as initially stated by TPBank.

Employees at TPB identified suspicious SWIFT messages in time and contacted all parties involved. This prevented the transfer requests from being completed and the attempt to steal was halted.

BAE Systems stated that it did not have enough evidence to incontrovertibly attribute the hack but it said currently available evidence strongly suggested a connection to the group conducting other similar attacks.[8]

This attack represent an interesting case due to the months of cooperation between TPB and Kaspersky Lab that uncovered more and more tools hidden deep inside the bank's infrastructure. The second relevant characteristic is the persistence of the attackers: the attackers updated their tools in order to circumvent the latest security update released by Swift. Once the contact between the bank and Kaspersky Lab was established, the attackers somehow realized that the behavior of system administrators was not normal and soon after that they started wiping all traces of their activity. However, kaspersky Lab managed to collect and build a rough timeline of some of their operations, as we can see in figure 8.

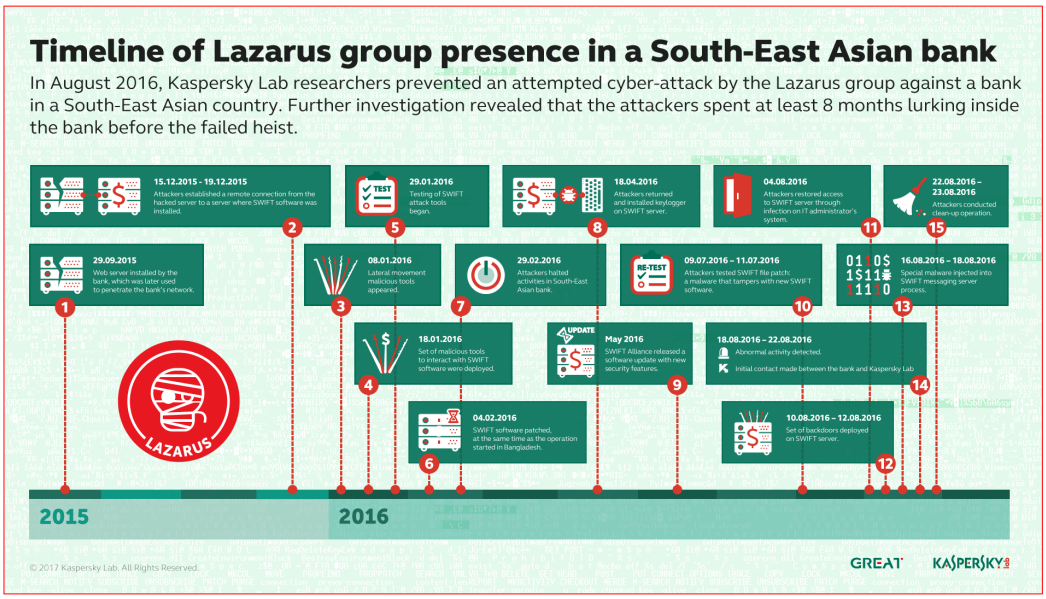

Figure 8: Timeline of the Tien Phong Bank attack according to Kaspersky Lab.

The investigation suggests attacker activity around 2016-02-04 14:07:07 (UTC) that was also the date of the Bangladesh cyberheist. It was also discovered that the malware used in the two attacks present some visible similarities.

Due to the age of the breach inside the bank it was not very clear how the attackers initially breached the bank. However, what becomes apparent is that they used a web server located in the bank to connect via Terminal Services to the one linking to SWIFT connected systems.

The web server installation was quite new: it had hosted the company's new website for just a few months before it was compromised. The bank even contracted a pentesting company to do a security assessment of the new website which was ongoing when the attackers breached the server.[9]

Security researcher Christiaan Beek found the code TPBVVNVX - which is the SWIFT code for the Tien Phong Commercial Joint Stock Bank in Hanoi - hidden in multiple parts of the malware used for the attack. He also noticed that there were more SWIFT codes in the code:

- UOVBSGSGXXX - United Overseas Bank Ltd, Singapore
- ANZBAU3MXXX - Australia and New Zealand Banking Group Ltd, Melbourne, Australia
- BOTKJPJTXXX - Bank of Tokyo-Mitsubishi UFJ Ltd, Tokyo, Japan
- MHCBJPJTXXX - Mizuho Bank Ltd, Tokyo, Japan
- CZNBKRSEXXX - Kookmin Bank, Seoul, South Korea
- UNCRITMMXXX - Unicredit S.P.A., Milan, Italy
- ICBKVNVNXXX - Industrial and Commercial Bank of China, Hanoi branch, Vietnam
- ICBKUS33XXX Industrial and Commercial Bank of China, New York branch, United States

Other than the above-mentioned behaviour, the malware reads the SWIFT messages and checks if the sender of the message is one of the listed banks. Once it finds these messages, it reads their information and then it can manipulate these messages. This information suggest that at a certain point one of the intent of the attack would have involved these potential targets.[10]

1.2.4 The Bank of Bangladesh, Bangladesh - February, 2016

On February 4, 2016 an attacker accessed the Bangladesh Bank's SWIFT payment system and attempted to transfer $951m from the bank's account to accounts in the Philippines. As of now, $81m are still unaccounted for.

The cyber attack on the Bank of Bangladesh was one of the largest heists and most calculated and sophisticated attacks against SWIFT systems to date. Investigations found that the attack had been patiently executed over a long period of time, in fact evidence discovered by subsequent investigation has shown that the targeting of banks in Bangladesh began as early as October 7, 2014.

The FBI's investigation, including its analysis and examination of digital devices and electronic evidence received from Bangladesh Bank, identified four key accounts used to target and infiltrate Bangladesh Bank: watsonhenny@gmail.com, yardgen@gmail.com, and two accounts connected to them, rasel.aflam@gmail.com and rsaflam8808@gmail.com. The spear-phishing emails from each of those four accounts were nearly identical and read as follows:

> I am Rasel Ahlam.
>
> I am extremely excited about the idea of becoming a part of your company and am hoping that you will give me an opportunity to present my case in further detail in a personal interview.
>
> Here is my resume and cover letter. Resume and cover letter http://www.[DOMAIN REDACTED].com/CFDOCS/Allaire_Support/rasel/Resume.zip
>
> Thank you in advance for your time and consideration.

These links may have hosted the malware that allowed the subjects to gain initial access to the computer network of Bangladesh Bank, but it is not possible to very this assertion anymore. Another piece of evidence is that stored in watsonhenny@gmail.com's address book, by June 24, 2015, the account had thirty-seven email addresses of personnel at Bangladesh Bank saved in it.

On January 29, 2015, the account yardgen@gmail.com sent 10 email messages to sixteen different email addresses of employees of Bangladesh Bank. Each of those messages purportedly sought an employment opportunity using the email quoted above. On February 23, the same account sent other two email messages to ten recipients at Bangladesh Bank.

On August 11, 2015, the account rsaflam8808@gmail.com sent a message to another Bangladesh-based bank (not Bangladesh Bank). The content of this email was the same as the emails sent by yardgen@gmail.com to

employees of Bangladesh Bank. This information highlight the broader scope of the hacking campaign. On August 11 and 12, 2015, the account rasel.aflam@gmail.com sent twenty-five spear-phishing messages to employees of multiple Bangladesh-based banks using the same email quoted.

After the heist of Bangladesh Bank, forensic review and analysis revealed that at least three Bangladesh Bank computers had attempted to download the file.

Since March 2015, the attackers had moved within the Bangladesh Bank network and had saved a file that was a backdoor that communicated over a custom binary protocol designed to look like "TLS" traffic. That malware was capable of performing file transfers, creating .zip archives, and executing certain files. This indicate that most of the later phishing emails were sent in order to ease the harvesting of credentials and to gain higher access to the systems of Bangladesh Bank. This malware is a variation of the MACKTRUCK backdoor.

The sophistication of this attack can be figured just by looking at how many malware were developed and used in order to gain access to the SWIFT environment. Other than the MACKTRUCK backdoor, other malware were used such as NESTEGG, Brambul and evtdiag.exe.

Attackers also employed trojanized PDF reader and software that prevented details of the transactions from being printed out on the bank's printer, thus delaying the bank's discovery of the fraud. The software specifies the printer model, which is "HP LaserJet 400 M401".

On January 29, 2016, days before the fraudulent transfers were made, the attackers engaged in a number of lateral movements throughout the network, including from the computer where they had installed a file that communicated by mimicking TLS traffic. One of those moves was to Bangladesh Bank's SWIFTLIVE system. That system was the core component of Bangladesh Bank's SWIFT processing environment. It used the SWIFT Alliance Access application, which was a customer-managed gateway to the SWIFT network that transmitted and received messages from other banks that create and confirm financial transactions. As the application received SWIFT messages, it would record local copies of the messages, including by formatting and printing those messages to files or a printer and by entering information associated with them in a separate database.

As the hackers tried to move onto the Bangladesh Bank computer hosting the SWIFTLIVE system, they made at least four attempts to login to it. The subjects had successfully deleted some evidence of their attempts to log-in to Bangladesh Bank's SWIFTLIVE system but left some evidence that was later found during the forensic examination. Significantly, one of those log-in attempts (that presumably was not successful) used the name of a specific currency exchange business in South America. The mentioned South American currency exchange had already been targeted by the same attackers, and thus the attempt to use credentials associated with it was likely an error by the hackers who were conducting or managing multiple intrusions at the same time and remotely accessing Bangladesh Bank's computer systems.

Once access to SWIFT systems was obtained, the attackers monitored employee behaviour, stole user credentials, and deployed specifically-designed malware. The malware targeted the SWIFT Alliance Access application, bypassed its security controls, and removed evidence from printed SWIFT messages, as explained before. A summary of the modus operandi can be observed in figure 9.

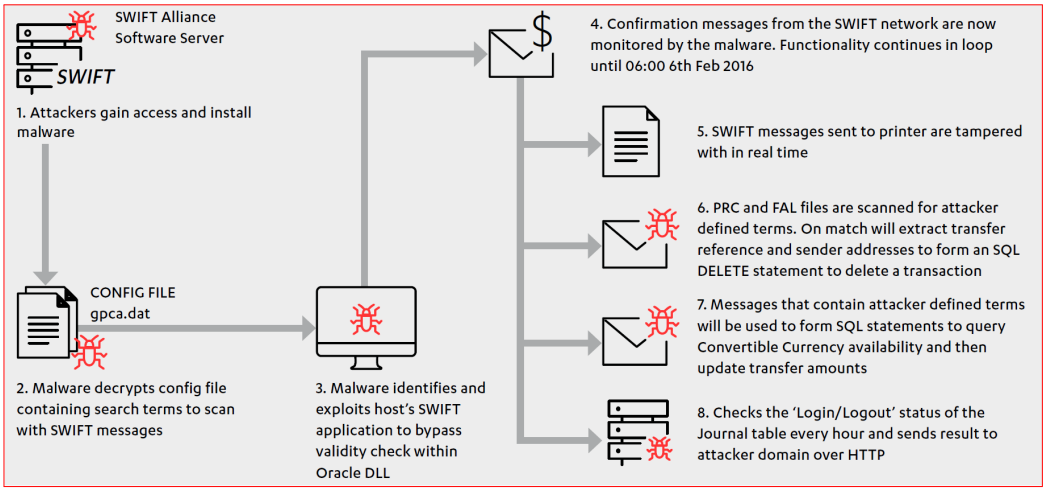

Figure 9: Bank of Bangladesh Hack

In order to grant the ability to execute database transactions, the malware targeted a specific module that was responsible for managing some of the core functions of the database. In fact, the malware enumerates all processes, and if a process has the module liboradb.dll loaded in it, it will patch its memory.

The patch will essentially jump some important check, such as a key validity check or authorisation success check. A brief summary of this process is represented in figure 10.

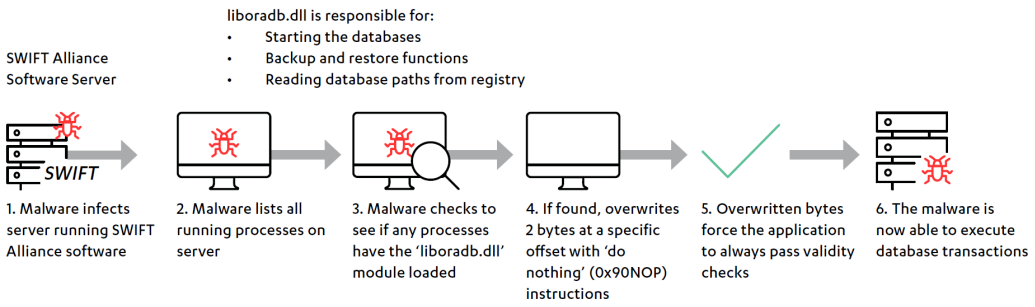

Figure 10: How the malware exploited liboradb.dll

On February 4, a total of 35 SWIFT transactions worth $951,000,000 were made to the Federal Reserve Bank of New York asking the bank to transfer the funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.

Thirty transactions worth $851 million were flagged by the banking system for staff review, but five requests were granted; $20 million to Sri Lanka and $81 million lost to the Philippines.

This money was laundered through casinos and some later transferred to Hong Kong.

The $20 million transfer to Sri Lanka was intended by hackers to be sent to the Shalika Foundation, a Sri Lanka-based private limited company. The hackers misspelled "Foundation" in their request to transfer the funds, spelling the word as "Fundation". This spelling error gained suspicion from Deutsche Bank, a routing bank which put a halt to the transaction in question after seeking clarifications from Bangladesh Bank.

The money transferred to the Philippines was deposited in five separate accounts with the Rizal Commercial Banking Corporation (RCBC); the accounts had all been opened a year earlier in May 2015, but had been inactive with just $500 sitting in them until the stolen funds arrived. The funds were then transferred to a foreign exchange broker to be converted to Philippine pesos, returned to the RCBC and consolidated in an account

of a Chinese-Filipino businessman. On February 8, 2016, Bangladesh Bank informed RCBC through SWIFT to stop the payment, refund the funds, and to "freeze and put the funds on hold" if the funds had already been transferred. The message was received by RCBC only a day later due to the fact that it was the Chinese New Year, a non-working holiday . By this time, a withdrawal amounting to about $58.15 million had already been processed by RCBC's Jupiter Street (in Makati City) branch. RCBC was fined for its non-compliance with banking laws and regulations in connection with the bank robbery.[11][12][13]

1.2.5 Unnamed Ukrainan bank - 2016

Details regarding the compromise of an unnamed Ukrainian bank are limited, though it was reported that $10,000,000 was stolen and that the attack was similar to that of the Bank of Bangladesh.

The Information Systems Audit and Control Association reported that the theft had occurred via the SWIFT system however it did not name which bank had hired some of its members to conduct the investigation.[14]

It was further reported that this attack was only one of many that the Ukraine and Russia had experienced, involving dozens of banks (mostly in Ukraine and Russia), resulting in the loss of "hundreds of millions of dollars".

It's not clear if the Ukrainian bank heist involved the same malware or was the work of the same hackers that attacked the Bangladesh Bank as the threat-intelligence firm iSight Partners, a FireEye division, notes that the Ukraine hack may be the work of a different cybercrime organization that used malware to steal an estimated $25.5 million from Russian bank accounts.[15]

1.2.6 Polish Financial Supervision Authority (Komisja Nadzoru Finansowego) - January, 2017

In early February 2017, the Polish Financial Supervision Authority (KNF) took its systems offline after discovering that malicious code had been placed on its webserver and was being used to redirect designated targets to malicious payloads. Subsequent public reporting indicates that multiple Pol-

ish banks have confirmed that they had identified malware on their systems. Based on further analysis, it is believed that this campaign was more widespread and was intended to primarily target financial institutions.

On Feb. 3, 2017, InfoSec news blog badcyber reported that multiple Polish commercial banks were allegedly infected with malware. The initial investigation suggested that the initial infection vector occurred via the KNF website (figure 11). FireEye iSIGHT Intelligence confirmed that unauthorized code was being hosted in a JavaScript file on the KNF domain, which was being used to redirect visitors to an exploit kit landing page.

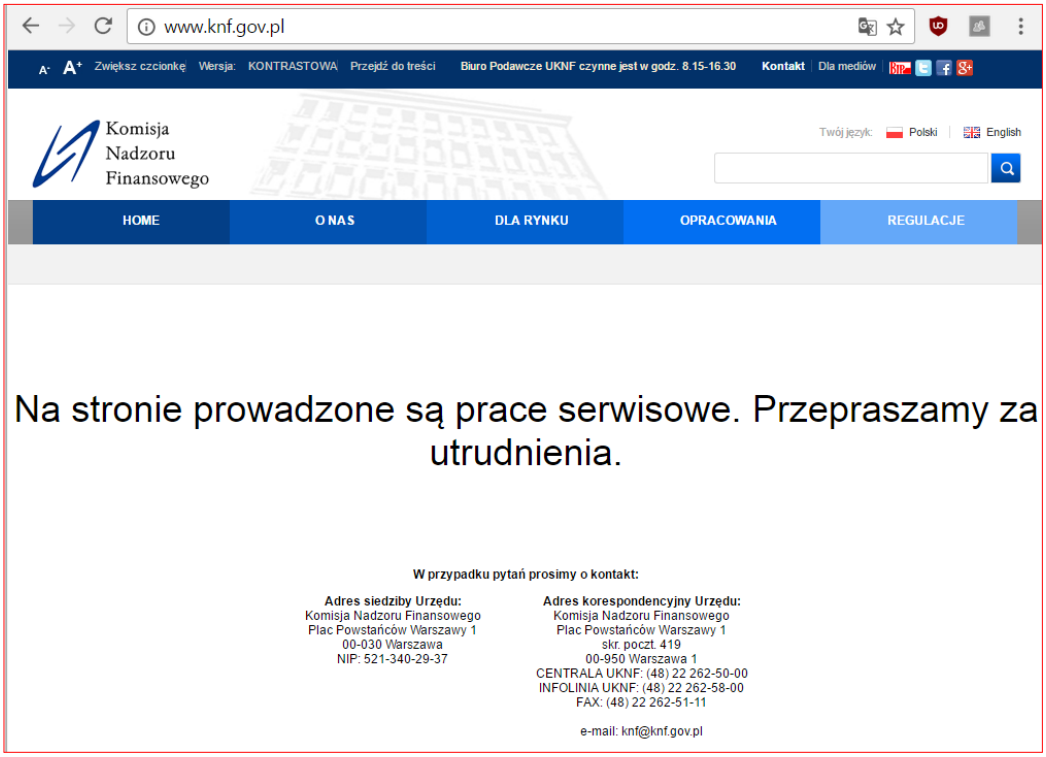

Figure 11: http://www.knf.gov.pl

A whitelist of IP addresses observed in conjunction with the KNF incident specified which individuals would receive the designated payload. The whitelist contained IP addresses associated with 104 organizations, many of which are in the financial sector. This whitelist suggests that the threat actors were highly selective in choosing their targets. Most of the whitelisted

IP addresses correspond to Polish financial institutions.

Based on indicators gleaned from open-source reporting, malware associated with the KNF compromise has previously been observed in past SWIFT-related intrusion activity. Given this similarity, it is plausible that KNF intrusion activity shares at least some operational overlap with the SWIFT manipulation attacks widely reported in 2016; however, attribution of this activity is not conclusive.[16]

There is currently no evidence of monetary loss associated with affected Polish banks. However, one media report claimed that a large amount of data was stolen from one Polish financial institution. the nature of the data that was stolen is unclear.[17][18][19]

1.2.7 Russian bank - 2017

The Russian central bank reported the in 2017 unknown hackers stole 339.5 million roubles, roughly $6 million, from a Russian bank via SWIFT system.

The hackers had taken control of a computer at a Russian bank and used the SWIFT system to transfer the money to their own accounts. The spokesman of the central bank declined to name the bank or provide further details but he quoted Artem Sychev, deputy head of the central bank's security department, as saying this was "a common scheme". In fact, it was reported that during 2016 hackers stole 2 billion rubles from accounts that banks keep at Russia's central bank. During 2016 the attackers tried to steal 5 billion rubles, but the central banking authority managed to stop them and redirect some of the funds. The total loss amounted to 2 billion rubles.

The hackers targeted commercial banks, but they also stole cash from their clients, the central bank reported. At this time, it's unclear who has attacked Russian banks.

Also, at the end of 2017, hackers tried to steal 55 million rubles ($940,000) from Russian state owned bank Globex using the SWIFT system. The bank spotted the attack and was able to prevent the attackers from stealing all the funds they had sought: the hackers only withdrew around $100000.[20][21][22]

1.2.8 The Far Eastern International, Taiwan - October, 2017

In October 2017 an attack was carried out against the Far Eastern International Bank. During the heist, attackers used malware which has been linked to multiple attacks on financial institutions around the world. This malware was used to gain access to and move through the bank's internal network in order to infiltrate SWIFT systems. Attackers then compromised employee credentials and used this information to authenticate to the SWIFT Alliance Messaging Hub and issue a total of $60,100,000 worth of fraudulent transactions. By the time staff noticed the weird transactions, they had already been wired to banks in the US, Cambodia, and Sri Lanka. Although it was initially understood that $500,000 was lost, the Financial Supervisory Commission reported that the final amount lost by Far Eastern Bank was $160,000.[23]

Following an investigation, it was found that the bank's security posture was not in line with the requirements outlined by Taiwan's banking law. As a result, Taiwan's financial regulator fined the Far Eastern International Bank $266,524, raising the total financial loss of the incident to $426,524.[24]

Also in October, a cyber-security firm BAE Systems Plc said that a North Korean hacking group was likely responsible for a recent cyber heist in Taiwan.[25]

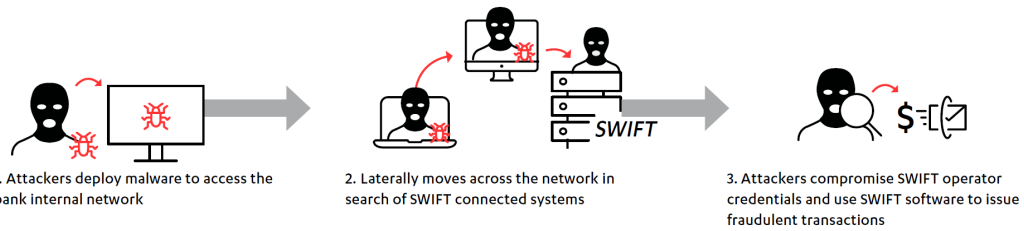

Figure 12: Far Eastern International Bank Hack

1.2.9 NIC Asia Bank, Nepal - October, 2017

NIC Asia Bank based in Kathmandu, one of Nepal's largest private-sector commercial banks, said attackers initiated $4.4 million in fraudulent money transfers through 31 transactions [26] via the SWIFT interbank messaging service from its accounts to accounts in six other countries, including the

United States, the United Kingdom, Japan and Singapore, according to the Himalayan News Service. After spotting the suspicious transactions, NIC Asia Bank informed Nepal's central bank, Nepal Rastra Bank, and NRB was able to recover $3.9 million, although $580,000 had already been released to overseas bank account. The SWIFT system of the Bank was hacked on 18th and 19th of October, during Tihar - aka Deepawali or Diwali - a five-day Hindu festival and one of Nepal's biggest holidays, from October 17 to October 21. The hack attack reportedly targeted NIC Asia Bank's Nostro accounts at Standard Chartered New York and Mashreq Bank New York. Banks hold Nostro accounts at another bank and in a foreign currency to facilitate foreign exchange transactions and trades. Roshan Kumar Neupane, deputy CEO at NIC Asia Bank, told PTI news agency that the bank took its SWIFT server offline immediately after spotting the suspicious transactions. After the transactions were discovered, NIC Asia Bank also commissioned KPMG India to conduct a digital forensic review, which it has shared with both NRB and Nepal Police's Central Investigation Bureau. But the results of the investigation reportedly failed to conclude if the theft resulted from an outside attacker or insider theft. An investigation into the heist launched by Nepal's central bank found that six staffers in NIC Asia Bank's SWIFT department had used a computer that was meant to be used only for SWIFT transactions for other purposes as well.[27][28]

1.2.10 City Union Bank, India - February, 2018

On Sunday, February 18, the Indian bank Kumbakonam-based City Union Bank announced that cyber criminals compromised its systems and transferred a total of $1.8 million.

The Indian bank confirmed that it has suffered a security breach launched international cyber-criminals and there is no evidence of internal staff involvement.

During the reconciliation process on February 7, it was found out that 3 fraudulent remittances had gone through our SWIFT system to corespondent banks which were not initiated from the bank. The operators immediately alerted the correspondent banks to recall the funds.

One transaction of $500,000 that was made through Standard Chartered Bank, New York, to a Dubai based bank was immediately blocked. A sec-

ond transfer of 300,000 euros ($372,150) was routed through a Standard Chartered Bank account in Frankfurt to a Turkish account, although the Turkish lender had blocked the transfer from being finalised. A third totaling $1 million was sent through a Bank of America account in New York to a China-based bank identified as Zhejiang Rural Credit Cooperative Union in Hangzhou, China.[29][30]

1.2.11 Banco de Chile - May, 2018

Banco de Chile, the country's second largest bank, on May 24 lost about $10 million due to fraudulent SWIFT wire transfers. The theft happened while the bank was dealing with hundreds of workstations and servers that suddenly stopped working.

Researchers with business risk intelligence firm Flashpoint say they've analyzed the malware used for the distraction portion of the attack against Banco de Chile. It's MBR Killer, a component of Buhtrap, a malware a-la NotPetya that first struck Russian banks in 2015. Buhtrap is a portmanteau of the Russian word "buhfalter" that means accountant, and trap. MBR Killer tampers with the master boot record, the first sector of a hard drive that the computer calls on before loading the operating system. The component renders the local operating system and MBR unreadable. The source code for Buhtrap leaked in early 2016, that means any group could be using it now to cause havoc. According to a screenshot of private IM conversations posted on a Chilean forum, the alleged "virus" crashed over 9,000 computers and over 500 servers. This malware didn't bother showing a ransom note and just wiped computer's MBRs, leaving them in a non-bootable state.

Banco de Chile General Manager Eduaro Ebensperger Orrego told the publication Latercera that it was eventually determined the initial attacks were likely a distraction. The real target was the bank's SWIFT system. The bank was able to stop some of the fraudulent transactions.

The attribution behind the Banco de Chile attack remains uncertain. "It is notable, however, that Chilean financial institutions were targeted entities by the Lazarus Group, which was linked to North Korea, during the compromise of the Polish Financial Supervision Authority website in 2017," Vitali Kremez, director of research, told Threatpost in an interview.

[31][32][33]

1.2.12 Cosmos Bank, India - August, 2018

Cosmos Bank is a 112-year old cooperative bank in India and it is the second largest in the country. Between August 10 and 13, 2018, over $13.5 million were stolen with an attack using multiple techniques, targeting both ATMs and the SWIFT environment.

On August 11, 2018, the bank's internal and ATM infrastructure was compromised. The exploit involved multiple malware leveraging a set of malicious libraries with a malicious ATM/POS switch in parallel with the existing Central and then selectively breaking the connection between the Central and the Core Banking System. The use of the malicious switch allowed the attackers to execute ATM withdrawals for over $11.5 million in 2849 domestic and 12000 international transactions using 450 cloned debit cards in 28 countries.

On August 13, 2018, the malicious threat actor continued the attack against Cosmos Bank by using the Cosmos bank's SWIFT credentials to successfully send three malicious transaction to ALM Trading Limited at Hang Seng Bank in Hong Kong amounting to around $2 million.[34][35]

Other attacks

In January 2018 a known group of hackers attempted to steal $110 million from the Mexican commercial bank Bancomext. That effort failed but just a few months later, a smaller yet still elaborate series of attacks allowed hackers to siphon off 300 to 400 million pesos, or roughly $15 to $20 million from Mexican banks.

Instead of using SWIFT, the attackers exploited the insecure network architecture within the Mexican financial system and poor security oversights in SPEI, Mexico's domestic money transfer platform run by central bank Banco de México, also known as Banxico.

The networks of targeted banks didn't have strong access controls, so hackers could get a lot of mileage out of compromised employee credentials. The networks also weren't well segmented, meaning intruders could use that initial access to penetrate deep into banks' connections to SPEI and, eventually,

SPEI's transaction servers.

The hackers also exploited flaws in how SPEI validated sender accounts to initiate a money transfer from a nonexistant source. They would then direct the phantom funds to a real, but pseudonymous account under their control and send a mule to withdraw the money before the bank realized what had happened. Each malicious transaction was relatively small, in the range of tens or hundreds of thousands of pesos. Attackers would have potentially needed to work with hundreds of mules to make all of those withdrawals possible over time.[36]

1.3 The attackers - APT38 a.k.a. Lazarus Group

North Korean group definitions are known to have significant overlap, and the name Lazarus Group is known to encompass a broad range of activity. Lazarus activities have been retroactively tracked back to 2007, under various names. For years, these activities were seen as acts of cyberterrorism and vandalism, since most of them systematically involved destruction of data and/or distributed denial of service attacks. The Lazarus group was clearly identified and named in the 2016 Novetta report "Operation Blockbuster". This report uncovered and attributed a large set of malware based on the analysis of the Sony Pictures Entertainment targeted attack. Attribution and tracking was made possible due to the group's habits of reusing huge chunks of code in most of their malware. This report showcased how active and diverse the group is: using more than 45 different home-developed malware families, Lazarus has been conducting destructive attacks but also advanced and persistent spying campaigns all over the world, making it worthy of the APT designation. TTP, arsenal and targets reveal that Lazarus is composed of at least three different subgroups: the Lazarus "core", aiming at disrupting activities and causing damage, Andariel, hacking for profit and intelligence, and Bluenoroff, motivated by financial gains. Uncovering its malware and activities didn't stop the Lazarus group from continuing its operations or renewing its arsenal.

APT38 targets financial companies mostly in Asia. Its first known operation took place in 2014 according to FireEye. This report doesn't clearly draw a link between APT38 and Lazarus subgroup Bluenoroff, which comes from

the fact that FireEye classify APT groups following its own strict rules and criteria. To remove any confusion, APT38 can be considered to be Bluenoroff, based on malware code overlaps and TTPs.

APT38 TTP (figure 13) resemble those of Lazarus subgroups, especially how they carry out their attacks and chose their targets. They have been focusing on attacking banks connected to the SWIFT network. They will most of the time infiltrate a bank network through vulnerable exposed servers, spend months gathering information, doing reconnaissance and moving laterally in the network until they find a way to steal money. Once the theft is complete, they will try to destroy all evidence. APT38 has its own toolset to maintain persistence, move laterally and manipulate SWIFT transactions. As mentioned in this report, their targets are diverse and worldwide. This group has also shown some amateurism and carelessness despite being quite sophisticated, which is a common trait amongst North Korean APT groups.

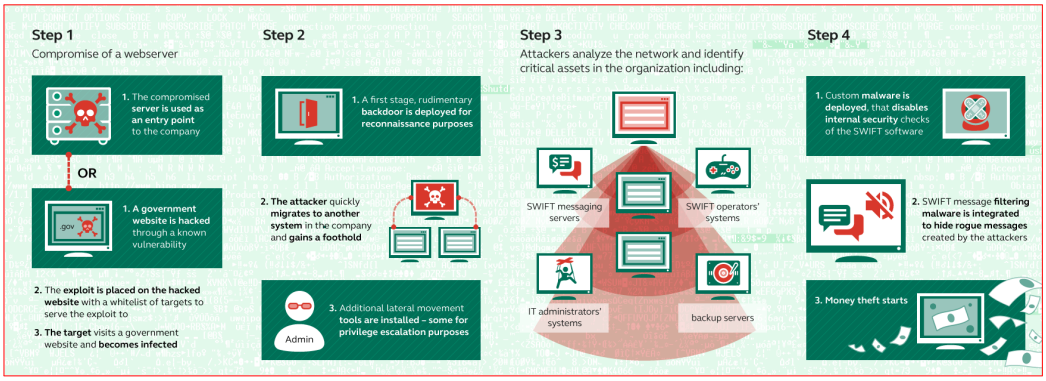

Figure 13: APT38/Bluenoroff tactics, techniques an procedures

North Korea has been targeted by multiple rounds of financial sanctions and restrictions. In 2017, the UN and the United States issued many resolutions and orders that had heavy negative impact on North Korea exchanges. To compensate, we have seen the Lazarus group focus on hacking financial institutions all around the world to steal money (figure 14). Even though disruptive attacks keep being conducted, it is clear that Lazarus prefer heists involving big sums of money. Likewise, spying operations are still being conducted by APT37.

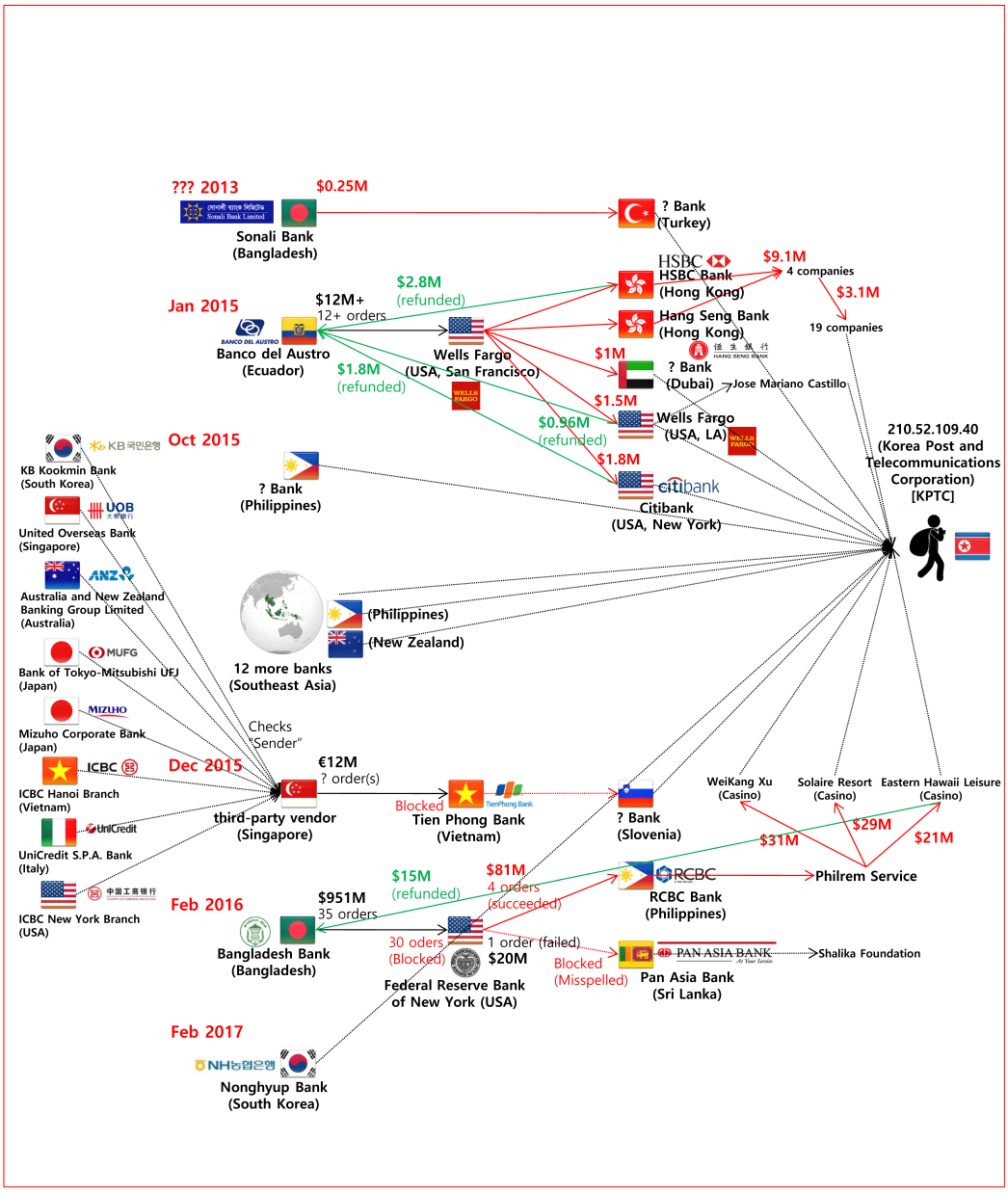

Figure 14: Swift Hacks

Most bank attacks are carried out by the Bluenoroff subgroup, while ATM attacks are usually attributed to Andariel. However, Lazarus members have recently been focusing on hacking cryptocurrency businesses, with a partic-

ular emphasis on South Korean exchanges. These attacks are very profitable and most of the time quite unsophisticated, making them the perfect way for stealing money rather than hacking banks and ATMs.

It's important to remember that much of the intelligence available on North Korea is dated and may not accurately reflect the regime's current capabilities. Moreover much of the intelligence available on North Korea comes from U.S. or South Korean military or agency reports. These reports omit details that are likely classified, such as specific IP addresses and individual actor information and, especially for South Korea, they may contain biased information. Obtaining details on North Korea's cyber warfare capabilities is not an easy task. It is easy to understand why by examining the few known cyber capabilities of North Korea's regime and how the country maintains secrecy in these matters.

The Democratic People's Republic of Korea (DPRK), known in the West as North Korea, is a unique country with a military-focused society and an unconventional technology infrastructure. Due to North Korea's global interactions, its cyber warfare capabilities are of particular interest. According to a 2009 report by Major Steve Sin, an intelligence analyst, North Korean hackers have successfully penetrated U.S. defense networks more frequently than any other country that has targeted U.S. defense assets. In order for Westerners to understand the North Korean mindset, it is necessary to examine the key components of North Korean political and ideological thought. North Korea has two primary ideologies that provide context for the regime's motivations and activities: juche (ju-cheh) and songun (sun-goon). Juche is the official political ideology of North Korea. It was instituted in 1972 and is based on the ideologies of Kim Il-Sung, the founder of the DPRK. Juche emphasizes self-reliance, mastering revolution and reconstruction in one's own country, being independent of others, displaying one's strengths, defending oneself, and taking responsibility for solving one's own problems. North Korea's air-gapped intranet exemplifies this philosophy in the country's cyber infrastructure. The juche philosophy explains North Korea's disdain for outside cultural and political influence. Juche challenges North Koreans to contribute to the regime's chaju (ja-ju), a concept of national sovereignty and independence. Songun is North Korea's "military first" doctrine. Songun emphasizes the priority of the military in resource allocation and political and economic affairs. This doctrine stems from the belief that the military is vital for preservation of chaju. Understanding songun mindset gives context for

this potential threat actor's motivations. According to a 2013 Congressional report, the strategy established under former leader Kim Jong-Il focused on "internal security, coercive diplomacy to compel acceptance of its diplomatic, economic and security interests and development of strategic military capabilities to deter external attack". In recent years, one primary factor has heavily influenced the current state of North Korea's relations with other nations: the rise of the regime's leader Kim Jong Un. Kim Jong Un officially rose to power in April 2012, following the death of his father Kim Jong Il in December 2011. Following his rise to power, the regime reportedly expanded its labor camps, and more military resources were allocated to target those attempting to defect. Kim also executed his own uncle, a high-ranking official who did not share his ideals.

When it come to North Korean cyber capabilities and limitations there is an important point to highlight about the North Korean infrastructure. North Korea's cyber infrastructure is divided into two major parts: an outward-facing Internet connection and a regime-controlled intranet. North Korea's outward-facing Internet connection is only available to select individuals and is closely monitored for any activity that is deemed anti-regime. Individuals using the outward-facing Internet connection must be authorized. Common citizens are limited to using the Kwangmyong (gwang me-young), a nationwide intranet with no access to the world outside North Korea. Also, Koryolink, the country's only cellular phone network, is tightly controlled by the regime and cell phone data plans are not available to most users. Email is also regulated by the regime. The Korea Computer Center (KCC), North Korea's leading government research center for information technology, has a vested interest in Linux research and is responsible for the development of North Korea's national operating system, Red Star OS. The OS's design suggests it was developed with means for the regime to monitor user activity.

According to Alexa rankings, the three most visited websites in North Korea are kcna.kp, the official website of the Korean Central News Agency (KCNA); rodong.rep.kp, another North Korean news site; and naenara.com.kp, North Korea's official web portal. Naenara translates to "my country". In March 2013, there were reports that the Chrome browser was blocking Naenara.com.kp due to malware.

In order to manage such effort to monitor its citizens, North Korean cyber war and intelligence structure has develop a particular structure that can be

observed in figure 15

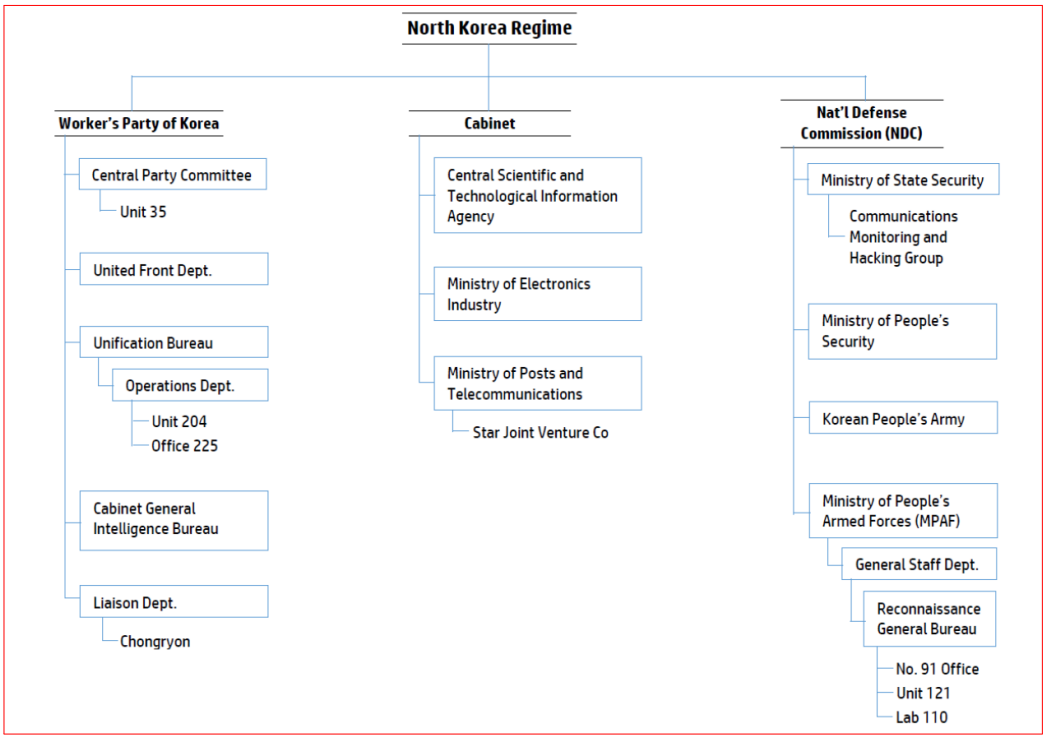

Figure 15: North Korean intelligence structure

North Korea's air-gapped networks and prioritization of resources for military use provide both a secure and structured base of operations for cyber operations and a secure means of communications. North Korea's hermit infrastructure creates a cyber-terrain that deters reconnaissance. Because North Korea has few Internet connections to the outside world, anyone seeking intelligence on North Korea's networks has to expend more resources for cyber reconnaissance. According to Kim Heung-kwang, a North Korean defector and former computer science professor, the regime has the following motivations for expanding its cyber warfare capabilities:

- Cyber capabilities are a cost-effective way to offset North Korea's lack of kinetic military prowess.
- North Korea's school systems place a strong emphasis on math, giving

the nation confidence in its programmers, cryptographers, and security researchers.

- In the modern warfare landscape, cyber capabilities are potentially more utilitarian than heavy artillery or aircraft.
- Cyber warfare capabilities provide a platform for espionage, psychological operations, and other forms of non-kinetic warfare.
- Considering the separatist nature of North Korea's infrastructure, cyber warfare provides a strategic advantage since outbound attacks are possible, but inbound attacks would have limited reach.
- Cyber warfare allows North Korea to leverage the Internet's inherent flaws for offensive purposes while maintaining its defenses, primarily via air-gapping its most critical networks from the outside world.

North Korea's attack and defense capabilities reportedly include the following cyber warfare and electronic warfare components: offensive cyber operations (OCO); computer network operations (CNO), which includes both computer network attack (CNA) and computer network exploitation (CNE); distributed denial of service (DDoS); satellite monitoring; drones; GPS jamming capabilities and deployment of electromagnetic pulse (EMP).

The basis of this capabilities is the early training and indoctrination. North Korea utilizes primary and secondary education and the university system to train its cyber warfare operators. According to reports by defectors, the regime seeks out children who show mathematical talent and sends them through rigorous advanced training. Science and technology students are expected to learn foreign languages, which may include Chinese, Japanese, and English. Student emails, chats, and web browsing activities are heavily monitored. Around age twelve or thirteen, chosen students are enrolled in accelerated computer courses at First and Second Geumseong Senior-Middle Schools. The successful students are then sent to Kim Il-sung University, Kim Chaek University of Technology, or the Command Automation University, traditionally known as Mirim University. The Command Automation University periodically chooses around 100 students for an intensive five-year course prior to their assignment to serve in cyber intelligence and cyber warfare capacities. Programs at the Command Automation University include command automation, computers, programming, automated reconnaissance,

and electronic warfare. Other students attend a two-year accelerated university program, then study abroad in Russia or China before they are assigned to a cyber-operator role. The elite cyber operators are given special incentives. For example, parents of students graduating from the cyber program with top scores are given the opportunity to live in Pyongyang; married cyber operators are given housing, a food allowance, and a stipend if operating overseas.

Other than executing cyber attacks, North Korea may strategically take credit for cyber attacks that were, in reality, launched by another entity. Whether the targeted entity blames North Korea for the attacks, or the regime simply takes credit for an attack that has not yet been attributed, several goals can come into play. First, to claim credit for an attack amplifies the impact of a show of force, particularly if South Korea is the target. This tactic can be used to stir sentiments in order to provoke a reaction. Second, North Korea may lay claim to responsibility for an attack that exceeds its capabilities in order to seem more technologically advanced and more capable. Third, any success, or the appearance thereof, enforces the juche ideal of regime self-sufficiency.[37][38]

2 The consequences

2.1 The aftermath

Since the disclosure of the first hacks, SWIFT has urged banks to protect themselves against the possibility of persistent, adaptive and sophisticated attacks. However, the long series of banks damaged by the attackers suggest that the warning was not taken seriously enough or that there was an insufficient effort from banks in securing their systems.

Consequently, SWIFT has taken extra measures to secure client banks, including sharing more information, supporting security audits and introducing tougher requirements for local bank computer networks. It is important to remember that none of the attacks succeeded in compromising the SWIFT network and its core messaging services so the effects on the SWIFT network are limited to the reputational damage and loss of trust in the network.

From the point of view of the consumer there is relatively little to lose from

cyberattacks on banks. Most regulations requires banks to refund customers if someone takes money from their account without authorization. Banks themselves instead have fewer assurances if a major cyberattack were executed. According to some experts these attacks could target bank processing systems and disrupt critical financial transactions needed to avoid margin calls, for example, triggering a default. Also, a cyberattack usually lead to a loss of confidence on that bank.

After the attacks SWIFT acted to limit the backlash. For instance, SWIFT said it had signed an agreement with Bangladesh's central bank to help it rebuild its infrastructure. SWIFT also agreed to provide technical assistance to Bangladesh Bank in its lawsuit against third parties involved in the heist. The firm stated it would continue to lend its support to international efforts to protect the global financial system from cyber attacks.

As for profits, the banks that collectively own SWIFT saw their profits fell by 31% as the organization increased its investments in information security.[39]

2.2 The investigation

The United Nations (UN) has opened an investigation into allegations against North Korea and its cyber attacks. Excerpts from a UN report, which suggested North Korea successfully raked in $2 billion from several attacks it carried out. UN Security Council also reported that North Korean state-backed hackers successfully breached at least five cryptocurrency exchanges in Asia between January 2017 and September 2018, causing $571 million in losses.

According to the panel of experts of the UN Security Council that investigated the cyberattacks carried out by the North Korea against multiple Member States the main objective of the targeted cyberattacks is to evade financial sanctions by illegally forcing the transfer of funds from financial institutions and cryptocurrency exchanges, laundering the stolen proceeds and generating income. The panel added that it has been targeted itself by cyberattacks.

The practical outcome of the UN investigation is represented by the actions taken by the affected states in order to counter the losses due to cyberattacks.

For instance the banking regulator of India has undertaken various preventive

measures which include:

- Issuing circulars on cyber security controls and on the controls that are required to be put in place for trade finance transactions to avoid misuse of the SWIFT ecosystem, advising the banks to implement controls for strengthening the security environment of the SWIFT infrastructure and to take steps to manage the operational risk surrounding the usage of the SWIFT system, in a time bound manner.
- Conducting special scrutiny of select banks to assess their operational control framework to safeguard against the risk of misuse of the SWIFT ecosystem.
- Issuing a circular to banks advising them to undertake a comprehensive audit of their SWIFT system covering the controls prescribed by the banking regulator.
- Sharing of market intelligence on the SWIFT ecosystem gathered from various sources with banks through the issuance of advisories, which include information on indicators of compromise affecting the SWIFT payment ecosystem and measures prescribed to check for compromise and plug these immediately.

Instead of relying on a passive response, the EU took more active measures. The Council of the EU established a framework which allows the EU to impose targeted restrictive measures, such as asset freezes or travel bans, in order to deter and respond to cyber-attacks. The EU has also begun implementing the Fifth Anti-Money Laundering Directive (AMDL5) which extends the scope of anti-money laundering rules to include cryptocurrencies.

Another investigation was launched by the United States. Based on details published in the DOJ complaint against North Korean programmer Park Jin Hyok (figure 16), an hacker from the Democratic People's Republic of Korea who worked as a member of the Lazarus Group, we know that APT38 and other cyber operators are associated with Lab 110, an organization subordinate to or synonymous with the 6th Technical Bureau in North Korea's Reconnaissance General Bureau (RGB). On 6 September 2018, the Government of the United States indicted Park Jin Hyok for engaging in a "wide-ranging, multi-year conspiracy to conduct computer intrusions and commit

wire fraud by co-conspirators working on behalf of the government of the Democratic People's Republic of Korea". According to the United States, Park "has travelled to China in the past and conducted legitimate IT work under the front company 'Chosun Expo' in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau". According to the United States, Park Jin Hyok and his co-conspirators also targeted and then executed the fraudulent transfer of $81million from Bangladesh Bank and engaged in computer intrusions and cyber-heists at many more financial services in the United States, and in other countries in Europe, Asia, Africa, North America and South America since 2015, with losses over $1billion.

WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. The front company – Chosun Expo Joint Venture, also known as Korea Expo Joint Venture – was affiliated with Lab 110, one of the North Korean government's hacking organizations. That hacking group is what some private cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

Figure 16: Park Jin Hyok most wanted poster

2.3 Customer Security Programme and Information Sharing and Analysis Centre

As a reaction to the cyber-threat landscape, SWIFT has implemented the Customer Security Programme (CSP). This programme requires all SWIFT customers to implement a number of controls defined by SWIFT's Customer Security Controls Framework (CSCF), to which customers must self-attest compliance. This framework outlines a collection of security controls to ensure a minimal baseline for security is in place across all customers' local SWIFT deployments.

Even if SWIFT customers are responsible for the security of their own environments, the security of the industry as a whole is a shared responsibility according to SWIFT. As a consequence SWIFT is committed to playing an important role in reinforcing and safeguarding the security of the ecosystem. From SWIFT point of view, this action represent one of the only option in order to safeguard the trust in the network.

The CSP is articulated around three mutually reinforcing areas. Customers will first need to protect and secure their local environment in order to safeguard themselves, it is then about preventing and detecting fraud in commercial relationships in order to safeguard network members and continuously sharing information and preparing to defend against future cyber threats.

The SWIFT Customer Security Controls Framework describes a set of mandatory and advisory security controls for SWIFT customers. The mandatory security controls establish a security baseline and must be implemented by all users on their local SWIFT infrastructure. SWIFT has chosen to prioritise these mandatory controls to set a realistic goal for near-term, tangible security gain and risk reduction. All controls are articulated around three overarching objectives: 'Secure your Environment', 'Know and Limit Access', and 'Detect and Respond'. The controls have been developed based on SWIFT's analysis of cyber threat intelligence and in conjunction with industry experts and user feedback. The control definitions are also intended to be in line with existing information security industry standards.

However, it is not possible to evaluate the effectiveness of this program because the document detailing the security requirement to implement - the "SWIFT Customer Security Controls Framework Detailed Description" - is not publicly available.

Fortunately, I was able to avail myself of a copy of the aforementioned document in its latest version, v2020.

Before diving into the security requirements it is important to observe the timeline of the implementation of such requirements. As we can see in figure 17, SWIFT adopted a change management process to evolve the controls framework. The process is designed to ensure that the SWIFT community has sufficient time (up to 18 months) to understand and implement the changes to the controls requirements. An emergency release may still be required in rare occurrences, to allow for the fix of critical and urgen issues.

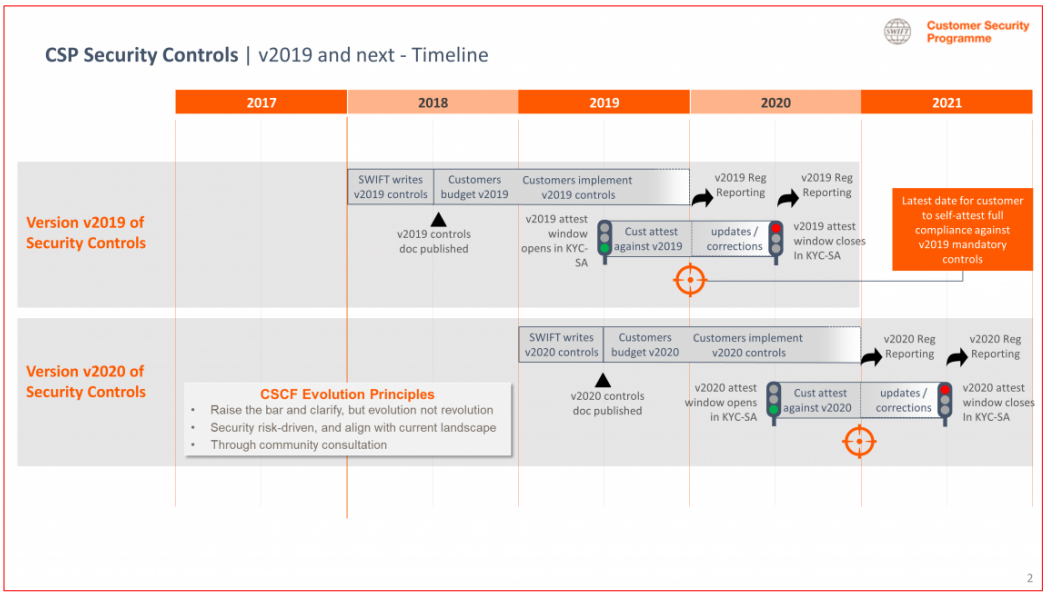

Figure 17: SWIFT CSP Security controls implementation timeline

The controls outlined in the CSP document represent general product-agnostic controls. Moreover, they should not be considered exhaustive or all-inclusive, and they do not aim at replacing a security and risk framework or compliance with the latest best practices and regulations. The controls are based upon three overarching framework objectives, supported by eight security principles. Objectives are the highest level structure for security within the user's local environment. The associated principles elaborate on the highest priority focus areas within each objective. The objectives and corresponding principles can be observed in figure 18.

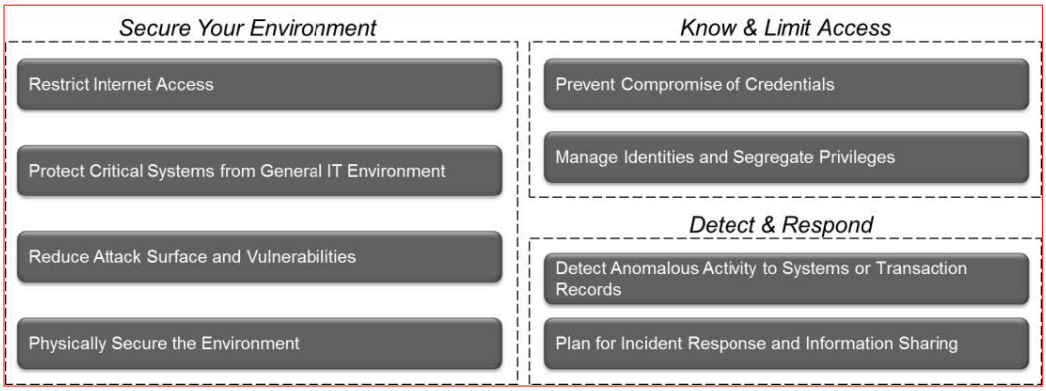

Figure 18: SWIFT CSP Framework Objectives and Principles

The 31 security controls (21 mandatory and 10 advisory controls as of 2020) are intended to help mitigate specific cybersecurity risks that SWIFT users face due to the cyber threat landscape. Within each security control, SWIFT has documented the most common risk drivers that the control is designed to help mitigate. While not yet mandatory, SWIFT encourages users to consider cyber risk management in the broadest possible terms, including beyond the scope of the user's SWIFT infrastructure and the SWIFT security controls. Organizations should incorporate SWIFT's controls into an ongoing cybersecurity governance and risk programme.

SWIFT has also published a guiding document to assist financial institutions in assessing their counterparty cybersecurity risk and incorporating this into their risk management framework. the document can be briefly summarized with the scheme presented in figure 19.

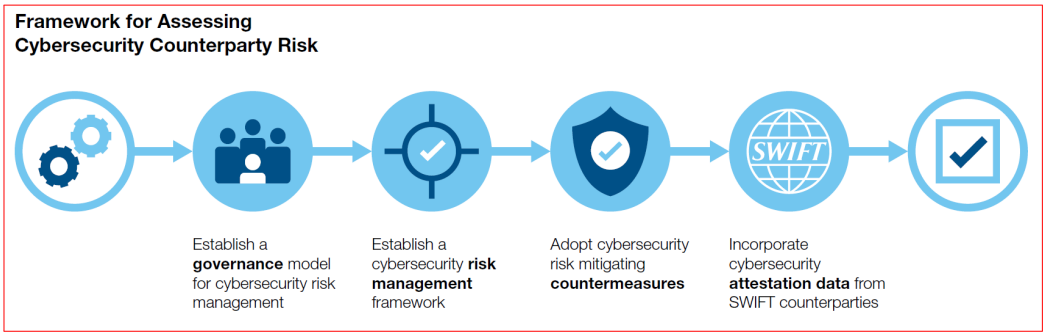

Figure 19: SWIFT counterparty cybersecurity risk

The security controls apply to the components defined by the scope previously highlighted in figure 3. The mandatory security controls are:

1. Restrict Internet Access and Protect Critical Systems from General IT Environment
    (a) SWIFT Environment Protection
    (b) Operating System Privileged Account Control
    (c) Virtualisation Platform Protection
    (d) Restriction of Internet Access
2. Reduce Attack Surface and Vulnerabilities
    (a) Internal Data Flow Security
    (b) Security Updates
    (c) System Hardening
    (d) Back Office Data Flow Security
    (e) External Transmission Data Protection
    (f) Operator Session Confidentiality and Integrity
    (g) Vulnerability Scanning
    (h) Critical Activity Outsourcing
    (i) Transaction Business Controls
    (j) Application Hardening
    (k) RMA Business Controls
3. Physically Secure the Environment
    (a) Physical Security
4. Prevent Compromise of Credentials
    (a) Password Policy
    (b) Multi-factor Authentication
5. Manage Identities and Segregate Privileges

   (a) Logical Access Control
   (b) Token Management
   (c) Personnel Vetting Process
   (d) Physical and Logical Password Storage

6. Detect Anomalous Activity to Systems or Transaction Records
   (a) Malware Protection
   (b) Software Integrity
   (c) Database Integrity
   (d) Logging and Monitoring

7. Plan for Incident Response and Information Sharing
   (a) Cyber Incident Response Planning
   (b) Security Training and Awareness
   (c) Penetration Testing
   (d) Scenario Risk Assessment

Every security control state the security goal to be achieved, the involved components, the risk drivers and implementation guidance. While going through the details of every control would be an interesting exercise it would also be pointless and a relative waste of time. In fact, anyone familiar with the NIST Cybersecurity Framework or the standard ISO 27002 would find the details of the controls very familiar. So familiar that SWIFT provide a table that maps the security controls against other security standard frameworks such as NIST, ISO 27002 ISO/IEC 27002 and the Payment Card Industry Data Security Standard (PCI DSS). Even if meeting the requirements from these industry standards does not automatically imply full compliance with the SWIFT security control the framework end up providing little or no added value.

For instance, we can observe in figure 20 how the first security control mentioned in the framework correspond to other framework's requirements.

SWIFT Control Objective	NIST Cybersecurity Framework v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
1.1 SWIFT Environment Protection Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	**Access Control (PR.AC)** **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate	**Network security management (13.1)** **13.1.3**: Segregation in networks	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data **Applicable Subsection(s):** 1.3
1.2 Operating System Privileged Account Control Restrict and control the allocation and usage of administrator-level operating system accounts.	**Access Control (PR.AC)** **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties	**User access management (9.2)** **9.2.3:** Management of privileged access rights	**Requirement 8:** Identify and authenticate access to system components **Applicable Subsection(s):** 8.1, 8.5

Figure 20: Extract of the mapping between SWIFT security controls and other industry standard

The second reaction after the cyber heist was the creation of the SWIFT Information Sharing and Analysis Centre (ISAC). The SWIFT ISAC portal stores all the information SWIFT had already been sharing with the SWIFT community through its portal called Knowledge Base on swift.com. This information includes malware details such as file hashes and YARA rules, Indicators of Compromise, as well as details on the Modus Operandi used by cyber-criminals. The SWIFT ISAC portal SWIFT aims to facilitate the community's access to actionable cyber-security threat intelligence, enabling the community to better defend itself against potential future cyber-attacks. However it's unclear if the ISAC portal represent only a rebranding of a previous portal or an active effort in intelligence gathering.[40]

3 The solutions

3.1 CSP and complementary solutions

The first solution implemented by SWIFT was the aforementioned CSP. Other than being redundant with other standards and regulations the proposed control should not be considered exhaustive or all-inclusive according

to own SWIFT statements. Therefore general attack methodologies can still be applied to the system as illustrated in figure 21 and 22. SWIFT systems are, and will remain, high-profile targets for all threat actors operating with financial motivations. Regardless of the implementation of standard or advanced security controls, there is still a high risk that these systems will have flaws that will be identified, targeted, and exploited by persistent threat actors. This is a consequence of the complex nature of the infrastructure deployed within financial institutions.

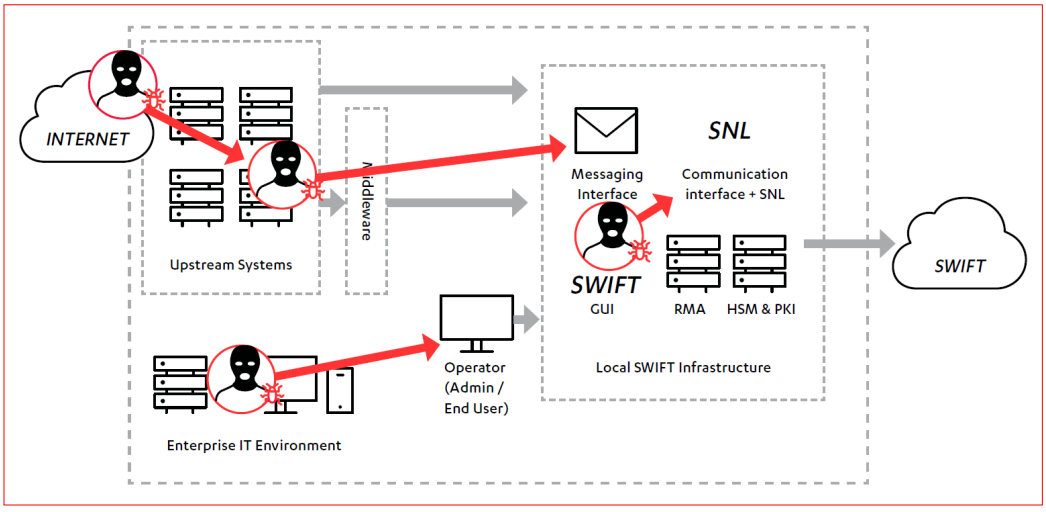

Figure 21: Attack Vectors due to weak security

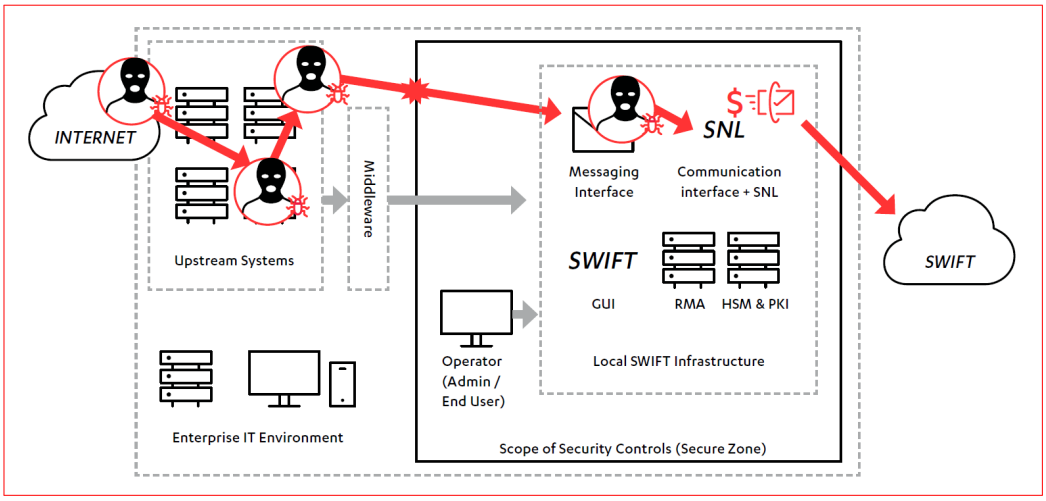

Figure 22: Attack Vector after implementing SWIFT CSP

SWIFT CSP compliance will ensure that the local SWIFT systems are hardened and isolated within a "Secure Zone". However, there will remain a number of upstream systems within financial institutions that can be used to action payments through SWIFT, which do not reside within the scope of SWIFT CSP's "Secure Zone". As such, financial institutions must predict, prevent, detect and respond. Ultimately, because SWIFT's CSP is a compliance challenge, which by nature is a rigid, linear process and because compliance does not ensure or imply security, as security itself is a fluid, cyclical process, the only viable solution is to builds on top of SWIFT CSP compliance to further strengthen the security posture of an institution as a whole. This methodology is rooted in establishing a strong understanding of how modern threat actors target financial institutions, mapping this understanding to the organization, and selecting appropriate preventative, detective and responsive measures. A 'point in time' approach to security will never succeed against an adaptive and persistent threat. The cyber-threat landscape is always shifting, and so only by turning the proposed methodology into a recurring practice can financial institutions and other organizations hope to secure themselves against future threats.[13]

3.1.1 Predict

It is key that financial institutions begin by understanding and mapping out the possible attack paths an attacker could take when attempting to compromise their enterprise network and local SWIFT infrastructure. This process begins at the SWIFT systems and works backwards towards the enterprise network perimeter in order to identify which systems communicate with the SWIFT infrastructure and the administration procedures surrounding these systems. Furthermore, all systems and applications deployed within the institution must be subject to frequent security assessment and penetration tests. A number of attempted (and successful) attacks on financial systems are never publicly reported, and as such organizations are advised to build trusted relationships with other local and international financial organizations to share information on tactics and tooling.

3.1.2 Prevent

Once these attack paths have been identified, an analysis of the steps an attacker would need to take to complete these paths should be ascertained. The controls surrounding each of these steps should then be assessed to confidently determine whether or not they would prevent such actions. This process should include security assessments of all controls along the path, as well as establishing an understanding of the legitimate use cases for all components. Financial institutions should also establish a strong understanding of which permissions and actions privileged users have access to, and how an attacker could subvert or abuse these privileges. If these actions are necessary and cannot be prevented, monitoring and detection of malicious behaviour should be implemented. A strong focus should also be placed on establishing controls that prevent malware execution. Furthermore, these controls should be redundant in the event one fails or is bypassed.

3.1.3 Detect

Recovery from these types of cyber heists is highly dependent on a timely response, facilitated by an efficient attack detection strategy. Discovering that a compromise has occurred when reading an end-of-day report is of little use. It is crucial that financial institutions implement robust logging of

all key servers within the environment and maintain visibility of servers and endpoint devices through endpoint detection and response (EDR) technologies. MWR further recommends that institutions adopt a threat hunting approach to detection and ensure that threat hunters are familiar with payment systems, as well as all known attacks against SWIFT systems. This should include prioritisation of the endpoints (including jump hosts) that are used by privileged users as these are the endpoints that are likely to be targeted by advanced threat actors during an attack.

3.1.4 Respond

When prevention fails, it is these detection and response capabilities that will ultimately determine the overall financial impact of an institution's local SWIFT infrastructure being compromised. Therefore, it is important that resources be placed in establishing a mature detection and response strategy surrounding your SWIFT deployment and its upstream systems. The main goal of this is to efficiently contain and recover from an attack. Regular incident response exercises should be conducted by financial institutions to ensure that the policies and procedures in place facilitate rapid response to an incident. This should include table-top exercises to test these procedures, as well as full incident response run-throughs based on SWIFT systems. Attack case studies such as the heist of the Bank of Bangladesh should be mapped to the organization's systems and the response team should work through this to establish if an investigation could have been rapidly conducted on their systems in the event of a similar attack.


Giacomo Minello

References

[1] Susan V. Scott and Markos Zachariadis. *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community*. 0th ed. Routledge, Oct. 30, 2013. ISBN: 978-1-315-84932-4. DOI: 10.4324/9781315849324. URL: https://www.taylorfrancis.com/books/9781317909538 (visited on 03/27/2020).

[2] N. Krishna and Ruma Paul Das. "Exclusive: Bangladesh probes 2013 hack for links to central bank heist". In: *Reuters* (2016). URL: https://www.reuters.com/article/us-cyber-heist-bangladesh-idUSKCN0YG2UT.

[3] *Another SWIFT Hack Stole $12 Million*. URL: https://www.bankinfosecurity.com/another-swift-hack-stole-12-million-a-9121.

[4] *Ecuador Bank Hacked — $12 Million Stolen in 3rd Attack on SWIFT System*. URL: https://thehackernews.com/2016/05/swift-banking-hack.html.

[5] "Exclusive: In Ecuador Cyber Heist, Thieves Moved $9 Million to 23 Hong Kong Firms". In: *Reuters* (May 25, 2016). URL: https://uk.reuters.com/article/us-cyber-heist-hongkong-exclusive-idUKKCN0YG2W9.

[6] "Special Report - Cyber Thieves Exploit Banks' Faith in SWIFT Transfer Network". In: *Reuters* (May 20, 2016). URL: https://uk.reuters.com/article/uk-cyber-heist-swift-specialreport-idUKKCN0YB0DO.

[7] *SWIFT Warns Banks: Coordinated Malware Attacks Underway*. URL: https://www.bankinfosecurity.com/swift-warns-banks-coordinated-malware-attacks-underway-a-9101 (visited on 03/27/2020).

[8] *Vietnamese Bank Blocks $1 Million SWIFT Heist*. URL: https://www.databreachtoday.com/vietnamese-bank-blocks-1-million-swift-heist-a-9105.

[9] *Lazarus Under The Hood*. URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf.

[10] *Attacks on SWIFT Banking System Benefit From Insider Knowledge*. May 20, 2016. URL: https://securingtomorrow.mcafee.com/blogs/other-blogs/mcafee-labs/attacks-swift-banking-system-benefit-insider-knowledge.

[11] *Two Bytes to $951m*. URL: https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html.

[12] *United States of America vs PARK JIN HYOK*.

[13] *SWIFT Threat Analysis*.

[14] *Bangladesh Bank Ends FireEye Investigation Into Heist*. URL: https://www.databreachtoday.com/bangladesh-bank-ends-fireeye-investigation-into-heist-a-9229.

[15] *Hackers Reportedly Steal $10 Million from a Ukrainian Bank through SWIFT Loophole - Jun. 25, 2016*. June 25, 2016. URL: https://www.kyivpost.com/article/content/ukraine-politics/hackers-steal-10-million-from-a-ukrainian-bank-through-swift-loophole-417202.html.

[16] *Mungurk/Apt_38*. URL: https://github.com/mungurk/apt_38.

[17] *Włamania do kilku banków skutkiem poważnego ataku na polski sektor finansowy*. URL: https://zaufanatrzeciastrona.pl/post/wlamania-do-kilku-bankow-skutkiem-powaznego-ataku-na-polski-sektor-finansowy/.

[18] Author badcyber. *Several Polish Banks Hacked, Information Stolen by Unknown Attackers*. Feb. 3, 2017. URL: https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/.

[19] *Polish Banks Infected with Malware Hosted on Their Own Government's Site*. URL: https://www.bleepingcomputer.com/news/security/polish-banks-infected-with-malware-hosted-on-their-own-governments-site/.

[20] "Hackers Stole $6 Million from Russian Bank via SWIFT System: Central Bank". In: *Reuters* (Feb. 16, 2018).

[21] "Unknown Hackers Stole $6 Million from a Russian Bank via SWIFT System Last Year". In: *Security Affairs* (Feb. 17, 2018). URL: https://securityaffairs.co/wordpress/69159/cyber-crime/russian-bank-swift-hack.html.

[22] "Russia's Globex Bank Says Hackers Targeted Its SWIFT Computers". In: *Reuters* (Dec. 21, 2017). URL: https://www.reuters.com/article/us-russia-cyber-globex-idUSKBN1EF294.

[23] Iain Thomson. *Hackers Nick $60m from Taiwanese Bank in Tailored SWIFT Attack*. Oct. 11, 2017. URL: https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/.

[24] "Taiwan's Far Eastern International Fined T$8 Million over SWIFT Hacking Incident". In: *Reuters* (Dec. 12, 2017). URL: https://www.reuters.com/article/us-far-eastern-fine-idUSKBN1E60Y3.

[25] Bae Systems Applied Intelligence. *BAE Systems Threat Research Blog: Taiwan Heist: Lazarus Tools and Ransomware*. URL: https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html.

[26] *NIC ASIA English Annual Report 2017-2018*. URL: https://www.nicasiabank.com/assets/backend/uploads/Annual%20reports/NIC%20Asia%20Bank/NIC%20ASIA%20English%20Annual%20Report%202017.18.pdf.

[27] *Report: Attackers Hacked Nepalese Bank's SWIFT Server*. URL: https://www.bankinfosecurity.com/report-attackers-hacked-nepalese-banks-swift-server-a-10437.

[28] *The NIC Asia Bank Is the Last Victim of the SWIFT Hackers*. Nov. 5, 2017. URL: https://securityaffairs.co/wordpress/65204/cyber-crime/nic-asia-bank-swift-hack.html.

[29] *City Union Bank Is the Last Victim of a Cyber Attack That Used SWIFT to Transfer Funds*. Feb. 19, 2018. URL: https://securityaffairs.co/wordpress/69268/cyber-crime/city-union-bank-hack.html.

[30] "India's City Union Bank CEO Says Suffered Cyber Hack via SWIFT System". In: *Reuters* (Feb. 18, 2018). URL: https://www.reuters.com/article/us-city-union-bank-swift-idUSKCN1G20AF.

[31] *Hackers Crashed a Bank's Computers While Attempting a SWIFT Hack*. URL: https://www.bleepingcomputer.com/news/security/hackers-crashed-a-bank-s-computers-while-attempting-a-swift-hack/.

[32] *Banco de Chile Wiper Attack Just a Cover for $10M SWIFT Heist*. URL: https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/.

[33] *Banco de Chile Loses $10 Million in SWIFT-Related Attack*. URL: https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075.

[34] *Cosmos Bank SWIFT/ATM Cyber Attack Detection*. Aug. 27, 2018. URL: https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/.

[35] *Police Investigate Cosmos Bank Hack*. URL: https://www.bankinfosecurity.com/police-investigate-cosmos-bank-hack-a-11379.

[36] "How Hackers Pulled Off a $20 Million Mexican Bank Heist". In: *Wired* (). ISSN: 1059-1028. URL: https://www.wired.com/story/mexico-bank-hack/.

[37] *The Lazarus Constellation*. URL: https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf.

[38] *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*.

[39] *Security Investments Consume SWIFT's Profits*. URL: https://www.bankinfosecurity.com/security-investments-consume-swifts-profits-a-9988.

[40] *SWIFT Launches the 'SWIFT Information Sharing and Analysis Centre'*. May 15, 2017. URL: https://www.swift.com/news-events/news/swift-launches-the-swift-information-sharing-and-analysis-centre.