CHRONOLOGY OF THE 2016 BANGLADESH BANK CYBER HEIST

I. ROSSENBACH

21.04.2020

RandoriSec

TLP WHITE

twitter: @secucrypt

ABOUT THIS CHRONOLOGY

- Relies on publicly available information

- whoami

TLP WHITE


SWIFT

SWIFT: Society for Worldwide Interbank Financial Telecommunication

Founded in 1973, cooperative society, headquarters in Belgium

2015:

+11 000 participants (banks, clearing houses, corporates…)

+212 countries

+15 million messages per day

Dominant position, *de facto* almost of a monopolistic nature

Main function: exchange of payment orders

SWIFT services:

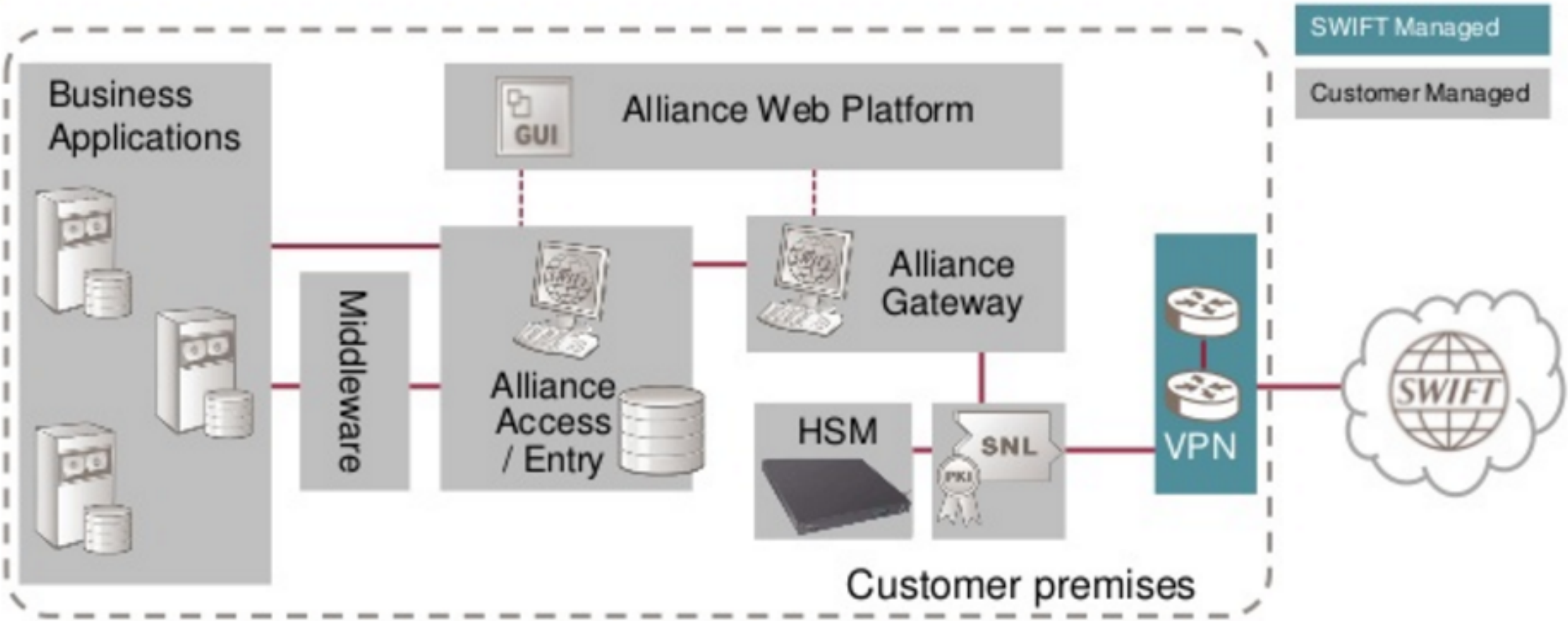
- InterAct:
Single transactions (XML) ~ SMTP

- FileAct:
File tranfers, bulk transactions, real time or store-and-forward ~ FTP

- Browse:
Secure browsing ~ HTTPS

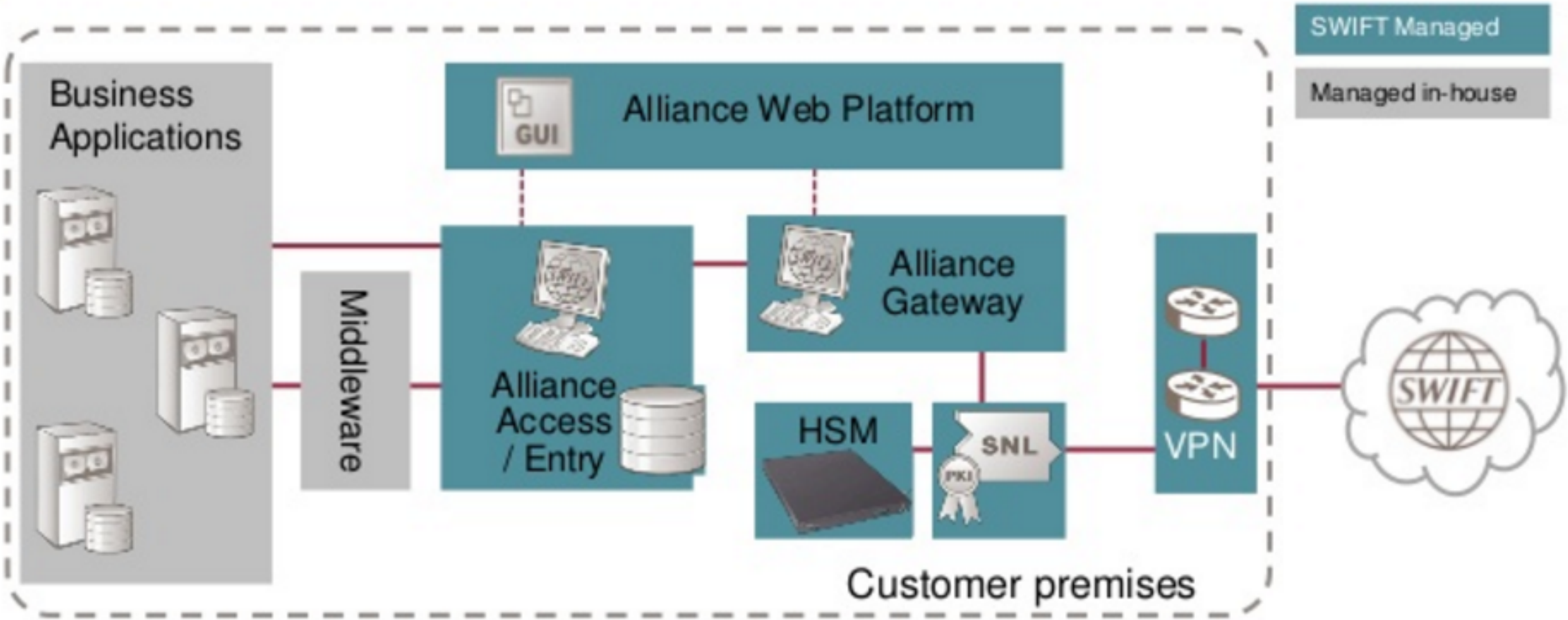
Typical SWIFT Infrastructure

High-level overview

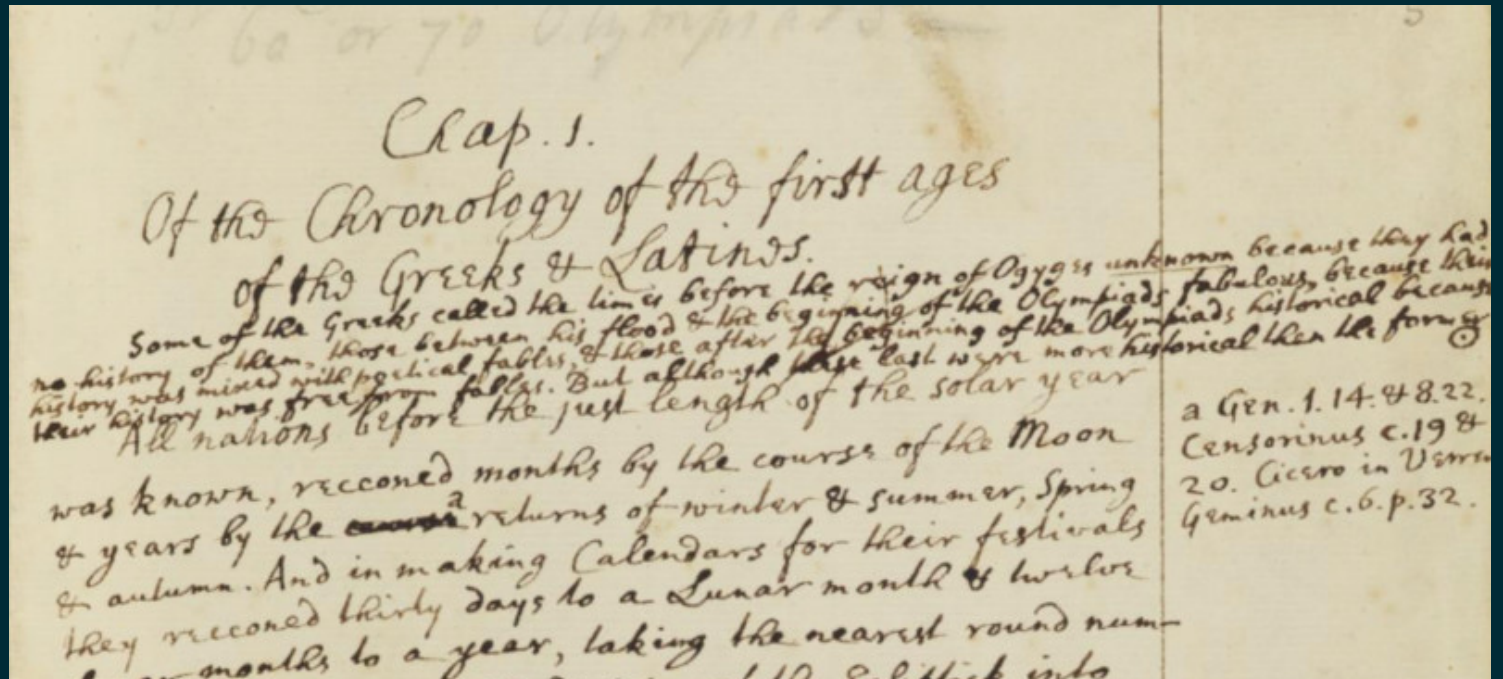


Alliance Managed Operations

High-level overview



CHRONOLOGY



Chap. 1.

Of the Chronology of the first ages
of the Greeks & Latins.

Some of the Greeks called the time before the reign of Ogyges unknown because they had no history of that: those between his flood & the beginning of the Olympiads fabulous, because their history was mixed with poetical fables, & those after the beginning of the Olympiads historical because their history was free from fables. But although the last were more historical then the former

All nations before the just length of the solar year was known, reckoned months by the course of the Moon & years by the returns of winter & summer, Spring & autumn. And in making Calendars for their festivals they reckoned thirty days to a Lunar month & twelve months to a year, taking the nearest round num-

a Gen. 1. 14. & 8. 22.
Censorinus c. 19 &
20. Cicero in Verr.
Geminus c. 6. p. 32.

At some time before 24 January 2016

Attackers steal credentials from a SWIFT operator of the Bangladesh Bank via spear phishing emails

They deploy 6 different kind of malwares

Between 24 January and 2 February 2016

Attackers reco of the internal Bangladesh Bank (BB) IT systems

They try several times to connect to SWIFT systems

They launch a tool in order to monitor SWIFT systems and erase some (unknown) database entries

On Thursday 4 February 2016, around 20h00

- Day before week-end in Bangladesh

- Most of BB employees left the office

Attackers issue fraudulent SWIFT transactions

The first transaction reaches the NY FED on Thursday 4 February around 10h00

$20 million from a BB account to an account located in Sri-Lanka

Then 34 other transactions are issued for around a billion dollars

Transactions contained anomalies:

- None had the name of the recipient bank

- Most had private individuals as recipient

- Were not in line with the “common” orders received from BB (on the past 8 month, 235 orders, 2 per day / None with private individuals as recipient)

According to the press, at the FED side:

- In the morning, they can find up to 100 transactions to process. In average, the FED processes $800 billion per day

- Most of the transactions are automatically processed

- In case of a problem, the team in charge checks that the SWIFT format is correct, that the sender is authenticated and that he isn't under US financial / money-laundering / terrorist sanctions

- These kind of transactions are handled by a team of 10 persons / bad communication with other departments

The 35 transactions received on 4 February are rejected by the FED because of a format anomaly (recipient bank missing)

Almost immediately, transactions are sent again, corrected

5 are then authorized, the others blocked in order to be verified
Verifications show that something is wrong...

The FED contacts the Bangladesh Bank via SWIFT's messaging system

The SWIFT message is sent on Friday around 04h00. At BB side, one of the malwares blocks this kind of messages

On *Friday 5 February 2016*, one day after the beginning of the attack, the Deputy head of BB was on call

He joins the office at around 10h30 and sees that none of the SWIFT confirmation messages were printed

After several tries to print the messages, he leaves the office at 11h15. Such printing problem did occur in the past. But in this case, the reason was a malware blocking the printing process

At 12h30, no one is anymore present at BB premises, and the cyber robbery isn't discovered

Friday 5 February 2016 (US), the FED checks all BB transactions

Some of the alerts were due to the presence of the word “Jupiter”, which is the name of a tanker and of a shipping company under sanctions related to Iran

But that was a coincidence: the address of one of the recipient banks, Rizal Commercial Banking Corp (RCBC, Philippines) is “Jupiter Street”, in Manila

The FED sends 2 other messages via SWIFT to BB: also blocked by the malware

On *Saturday 6 February*, the Deputy head of BB arrives to the office at 09h00

He tries again to print the SWIFT confirmation messages

BB figures out that the SWIFT platform doesn't start and that the logs indicate that a file is missing or modified

At 12h30 they manage to print the messages and see the fraudulent transactions. They also see the messages from the FED

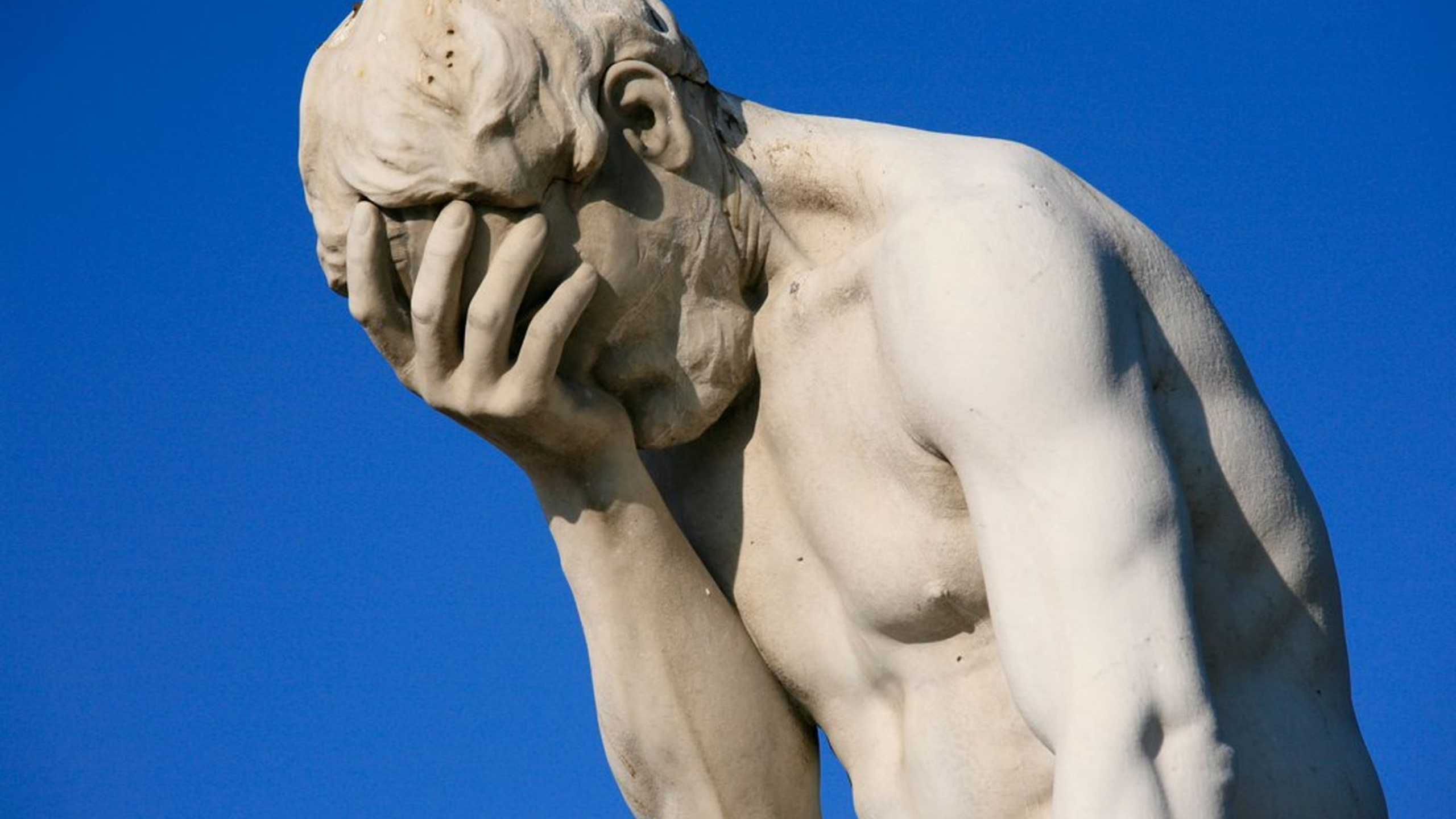
BB try to contact the FED, but they realize that they don’t have a direct contact...

They find an email on the FED website and send 3 messages

But this mailbox isn’t checked during week-ends

One of the messages says that their system has been hacked and asks to stop all transactions

BB also phone several times the FED, but as it's week-end, calls are unsuccessful...



On *Sunday 7 February*, the head of BB is informed. His deputy explains that the money is still in the pipe and that they will soon recover it

On *Monday 8*, BB recover its SWIFT infrastructure and sends a message “Top Urgent” to the FED explaining that the 35 sent transactions were fraudulent

On *Monday* evening in NY, 4 days after the heist, the FED informs the BB that the banks where the money was transferred were informed

$20 million sent to Sri Lanka were recovered, thanks to a detection by Deutsche Bank, who noticed a misspelling in a transaction

4 transactions for a total amount of $81 million were transferred to personal accounts opened with false identities at a Philippine branch of the RCBC bank

$22,7 million cash were withdrawn on Friday 5 February

On *Monday 8 February 2016*, BB send SWIFT messages to the RCBC asking to block the accounts. But...

On *Monday 8 February 2016*, BB send SWIFT messages to the RCBC asking to block the accounts. But...

... It’s a non-working day in Philippines. 4 quiet days for attackers.

On *Tuesday 9 February*, $58 million were already withdrawn

In the evening, RCBC informs BB that the accounts have been blocked... But there are only $68K remaining

RCBC will explain lately that the BB SWIFT message was not well formatted and not tagged as “Urgent” (reason why they only saw it on Tuesday evening)

Nevertheless, they manage to recover $18 million

The rest of the cash has been laundered in casinos (exempted from anti-money laundering laws)

The head of the branch will lately be fired, but he will explain that he received orders to open accounts under fake identities

On *7 March 2016*, BB announces that its account at the FED has been hacked and that money was stolen. They question / accuse the FED, who decline any responsibility

On *15 March*, SWIFT communicates mentioning “press articles”, reminds security essentials and states that they didn’t observe any security issue at their side

The same day, the BB governor resigns (money has not been recovered, and he delayed informing the government)

On *17 March 2016*, some details & confirmations are published: 35 transactions were made between 4 and 5 February, to recipient banks in Sri Lanka and Philippines

The recipient accounts were opened in May 2015: therefore, at least 9 month of preparation for this attack

LinkedIn reco to identify targets probably happened during summer 2015

4 valid transactions, total amount $81 million

$870 million were blocked or sent back:

- some because of the high amounts raised the suspicion of the Pan Asia Bank

- others because of a misspelling noticed by Deutsche Bank (“Shalika Fundation” instead of “Foundation”)

On *21 March 2016*, SWIFT asks its clients to check their level of security, and to strengthen it if needed (they provide a checklist)

Until this day, the main hypothesis was that it was about an internal fraud

From that day on...

On *25 April 2016*, BAE Systems publish an article about one of the malwares that could have been used

The malware (Windows platform) was retrieved from VT, where it had been submitted on 4 February (a couple of hours before the beginning of the attack)

This same day, SWIFT release a new version of its SAA platform, improving its integrity checking (checks performed each hour and not anymore once a day)

On *3 May 2016* SWIFT broadcast a new communication in which they say again that neither their infrastructure nor their network had been compromised

On May 12th, new SWIFT communication: mention of a new malware, mention of other targets

IOCs concerning a malware preventing the printing of fraudulent SWIFT messages are shared

BTW, what is an Indicator of Compromise (IOC) ??

It is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion…

An example?

Indicator of compromise:
{Tire marks on the right of the gate}

12 May 2016: BB accuses again the FED, as well as SWIFT's technicians. Both the FED and SWIFT reject these accusations

13 May: BAE Systems researchers say one of the malwares is similar to the one used against Sony in 2014 (Operation Blockbuster)

15 May: A Vietnamese bank, Tien Phong Bank, says they defeated an attack similar than the one against BB, performed via an external service provider. BAE systems also did talk about a similar malware

On *20 May 2016* : An information is published about Banco del Austro (Ecuador) which suffered a cyber robbery on 12 January 2015: $12 million stolen

Banco del Austro filed a claim against Wells Fargo and Citibank who released the money (Citibank did reimburse $1,6 million)

SWIFT say they were not aware and insists on the importance for their client to report any significant security incident

Report, share and communicate about security incidents

On *20 May 2016*: IOCs about malwares that try to modify the directory were acknowledgments are written or alter the MBR

24 May: SWIFT announce a new security program. SWIFT's CEO, says:

« The Bangladesh Bank hack was a "watershed event for the banking industry".
"There will be a before and an after Bangladesh. The Bangladesh fraud is not an isolated incident ... this is a big deal. And it gets to the heart of banking »

On *27 May 2016*: SWIFT launches a “Customer Security Program”

The five main issues this program will address are:

- Improve information sharing

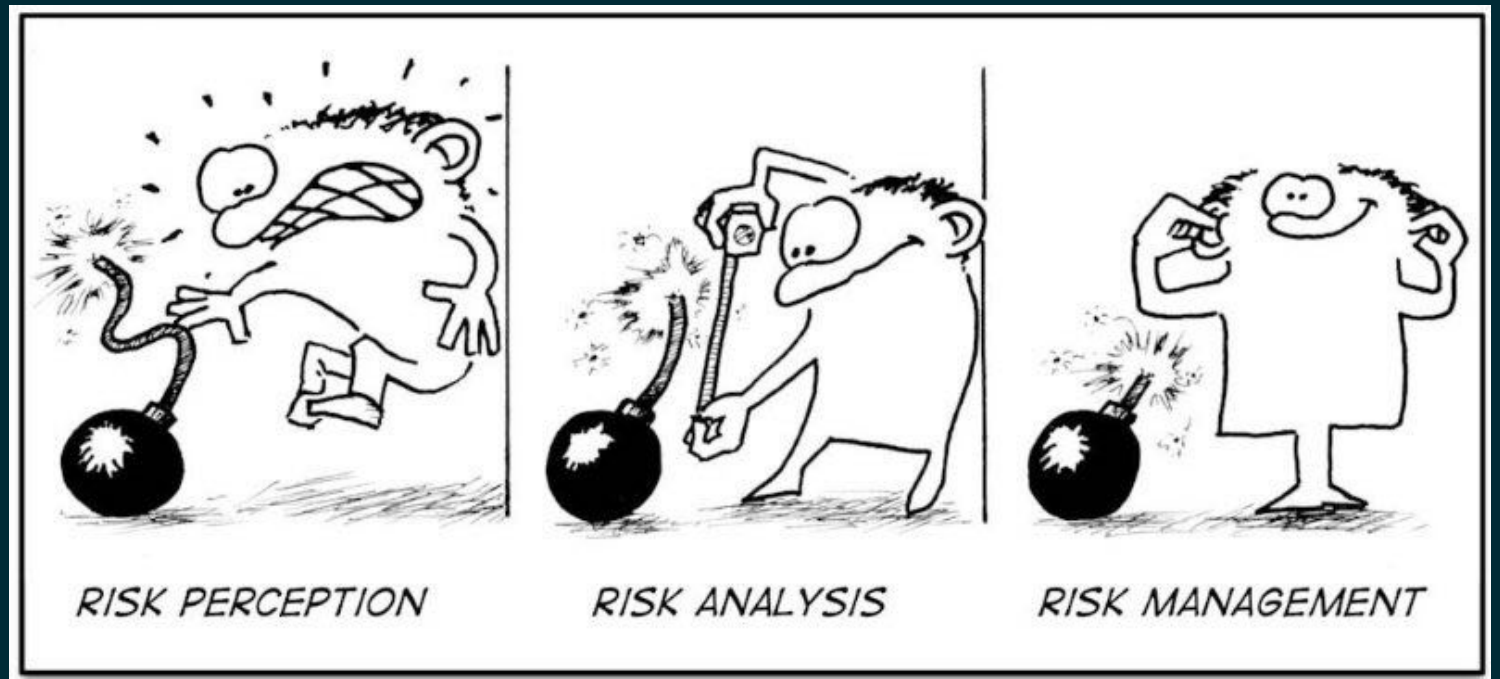
- Enhance SWIFT-related tools for customers

- Enhance guidelines and provide audit frameworks

- Support increased transaction pattern detection

- Enhance support by third party providers

Will that be another "soft" risk management framework ?



The mood seems to be more...

On *30 May 2016* : According to the head of the governmental investigation in Bangladesh, officials of the Central Bank could be implicated. An official report should be published

31 May : IOCs about spear phishing malwares. No explicit link to the BB heist, but mention of the fact that such a technic could have been used by attackers

17 June 2017: Some allege Russian and eastern European cyber-gangs are the authors of the heist, mainly because the Dridex malware would have been found...

But evidences & attributions based on tools are weak, and:

- There is a market for purchasing hacking tools

- There are also CaaS offers ("cloud" based)

- And cyber mercenaries…

On *14 July 2016*: New IOCs. Mention of Cobalt Strike, Mimikatz, Contopee, Nestegg, and containing YARA signatures

On *9 August 2016*: Release of an IOC with hashes which can be the sign of a successful compromission

12 August 2016: security bulletin for Alliance Access and Alliance Web Platform: Oracle vulnerability. Mandatory upgrade before 3 October.

30 August: IOCs that can be the sign of a compromission

On *30 August 2016*: SWIFT communicates to its clients that new attacks have been discovered in June. Some were successful

Targets were (likely) banks with weak security…

SWIFT explains that in case of security negligence, they could communicate toward partners and regulatory authorities

21 September 2016: SWIFT announce that a daily report will be transmitted to each client, with all the transactions received or emitted, as well as abnormal transfers. This report will be sent through a different channel than the transaction's one

21 September: according to Reuters, the "SWIFT Oversight Forum" a group of the 10 most important Central banks, leaded by the Central Bank of Belgium, asked regulatory authorities to control bank's security procedures, and thinks about new requirements

21 September: Possible *modus operandi* of attackers:

1/ Attackers compromise a client environment. Among the IOCs: phishing malware, update of Windows FW allowing remote connections, usage of legitimate softs for malicious purposes, remote control software, reco malware, malware reading SWIFT messages, etc.

2/ Attacker obtain creds allowing them to create, validate and submit SWIFT messages (from SWIFT servers or back-offices). Quoted technics are: social engineering (LinkedIn reco), shoulder-surfing, key logger, phishing, privilege escalation…

3/ Sending of fraudulent messages (using legitimate creds)

4/ Attackers remove some traces of fraudulent messages: increase the fraud detection time. Quoted technics are: malware deleting Windows events, SWIFT messages deleted from DB (MT950 end of day statements returned by the counterparty), prevent correct printing of messages / acknowledgments, moving acknowledgment messages… (?)

AND THEN SWIFT SAID...

AND THEN SWIFT SAID...

27 September 2016: SWIFT announce the publication of a list of mandatory security requirements, the already launched "Customer Security Programme" – 16 mandatory, 11 advisory – and of the associated assurance framework

Within 2017 self-assessments will be required, and from 2018 audits will be carried out

The results of the assessments (a % of compliant controls) will be available to counterparties upon request ("Know You Client" - KYC - approach), and could be communicated to regulatory authorities


WE ARE NOT
RESPONSIBLE
FOR
ZIPS, ETC

"SWIFT was, and still is, dominated by large Western banks, including Citibank, JP MORGAN, Deutsche Bank and BNP Paribas, that built the network decades ago. That contributed to the lack of concern over security, said the former directors, because the larger banks tend to have sufficient defenses to prevent criminals from hacking into their SWIFT systems."

"[A great] concern was the length of tenure of some members, which [...] did not encourage fresh thinking. At any time, a third of members had been there for "very long, perhaps too long"

(Reuters, 17 August 2016)

September 2016: several security companies (BAE systems, FireEye, Symantec…) talk about signs (TTPs, code similarities and geopolitical) and similarities with the 2014 Sony attack, and North Korea attacks. Lazarus group - Guardians of Peace (GOP)

5 October: SWIFT release an update of the *modus operandi*, with a description of fake SWIFT messages sent outside SWIFT network

11 October 2016: Symantec publishes an article about the "Odinaff" malware (using, in particular, malicious macros), used against SWIFT clients, but by another group. Links with Carbanak.

December 2016: Akbank... hacked

Possibly $120M stolen from the 4th largest bank in Turkey. Attackers are supposed to have created a "message partner", used by back-office functions, to create fraudulent payment messages.

Nevertheless, isn't believed to be Lazarus' work... (attribution bingo!)

16 January 2017: Information about 3 Indian banks (government-owned) where SWIFT infrastructures would have been “compromised”, allowing attackers to create fake trade documents. Goals, TTPs are unclear, as well as results.

23 January / 2 February : Some Central banks receive emails containing an attachment related to SWIFT and asking for

transfers (fraudulent).

August 2017:

Most of the attacks were stopped at different stages:

- some by SWIFT

- some by correspondent banks monitoring tranfers

- some by security community

Apparently, none by the victims of the intrusions themselves.

Attackers were able to reverse-engineer the SWIFT Alliance Access software as well as patches as new updates

Then, they were able to modify and update their malware accordingly

October 2017: Far Eastern International Bank, a Taiwanese bank victim of a hack. Funds were routed to accounts in Cambodia, Sri Lanka and the United States. US$60 million, most recovered.
2 persons arrested in Sri Lanka

A ransomware attack started in the network after the fraudulent payments were sent.

November 2017: NIC Asia Bank victim of a cyber robbery, resulting in a loss of Rs 60 million (400 million recovered)

December 2017 : Russia's Globex bank says hackers targeted its SWIFT computers. "Shane Shook, a cyber expert who has helped investigate some hacks targeting the SWIFT messaging network, said that at least seven distinct groups have been launching such attacks for at least five years, though most go unreported."

February 2018: India's City Union Bank suffered cyber hack via SWIFT system: 3 "fraudulent remittances", to accounts in Dubai, Turkey and China. Nearly $2 million, from which several transfers were blocked.

January - May 2018: Bancomext and Banco de Chile targeted and (US$11 million lost in the Chilean case).
Apparently, as in the Taiwanese hack, a "MBR Killer" was used during or after the attack.

April 2020: The Cybersecurity and Infrastructure Security Agency, a US agency, issues a "Guidance on the North Korean Cyber Threat" were the Bangladesh Bank heist is attributed to DPKR.


what
next?

PROBABLE SECURITY ISSUES

PROBABLE SECURITY ISSUES (1/2)

- Fundamentals: account management, hardening, VPM...
- Privileged account management
- Malware detection

- End user desktop security
- Network segregation
- 2FA authentication

PROBABLE SECURITY ISSUES (2/2)

- Email & web filtering
- Security monitoring, detection, alerting
- Regular pentests / redteaming

- Crisis management exercise / table top exercise
- Transaction business controls / detection / alerts
- 4 eyes process for most sensitive operations

CONCLUSION

CONCLUSION (1/3)

- The first conclusion is... that the story is not over yet: attack attempts are probably still ongoing, a lot of details still unknown, no attribution

- It is likely that attackers invested a lot, and it is obvious that they managed to combine high-level technical skills with an in-depth functional knowledge

- BB heist is the major cyber robbery ever known (in 2015, Carbanak, $500 million, but a lot of details remain unknown).

CONCLUSION (2/3)

- Missed alerts, alarms. Detection time is key (remember attacker efforts on hiding traces). Don't ignore applicative logs

- Beware of normalization of deviance / danger

- This case highlight the need to collect & conserve logs & traces that could serve as proof in a court case in case of a legal claim by a client previously hacked

- Share and communicate with pairs

- But be cautious with your *personal* communication: specific skills / positions in the organization are targets

CONCLUSION (3/3)

- According to the principle that **offense informs defense**: implement faulty / missing security controls and process

- Take advantage of the CSP for improving core security (it is *not* one more ISOlike compliance checklist)

- Don't forget back offices / business applications: will be the next generation of targets

- Regardless of preventive security measures in place, prepare reaction (DFIR, business incident handling process, crisis management, communication...)

¡ THANK YOU !

¿ QUESTIONS ?

iro@cryptosec.org | @secucrypt