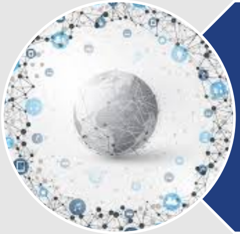
Securing Critical Infrastructures In The Financial Sector

Security Incidents in the Financial Sector and Lessons Learned

Incidents in the finance sector



Security Incidents

Bangladesh Bank cyber heist

- Bangladesh Bank's offices closed (February, 2016)
- Fraudsters intruded the SWIFT network of the bank and initiated US $1 billion to Federal reserve bank of New York out of which $850 million were blocked
- 3/35 fraudulent instructions -> transferring $101 million: $20 million traced to Sri Lanka & $81 million to Philippines
    - attack had its roots in the manipulation of the SWIFT Alliance Access software
    - one of the biggest cyber heist in history

Dridex take down operation and revival

- Dridex is a banking malware : most active 2015 - 2016
- At Oct 2015 UK's National Crime Agency (NCA) in cooperation with Federal Bureau of Investigation (FBI) & Europol coordinated a take-down activity by 'sinkholing' infected computers' traffic
- cybercriminals were believed to be based in Eastern Europe and target end users via documents delivered by e-mail addresses that seem legitimate.

➡

- £20M of estimated losses in the UK alone took place
- Declined but Dridex malware continues to evolve and remains a serious threat to end-users of financial services

Bank of Valetta Attack

- February 13, 2019 hack of Bank of Valetta
- malware planted on the bank's internal servers
- Security analysts believe that EmpireMonkey cybercrime group is believed to be behind this attack
- From a technical perspective, attackers used macros to copy wscript.exe to another file

- hackers transferred €13 million ($14.7 million) from the bank's internal systems to accounts in the UK, the US, the Czech Republic, and Hong Kong

ECB bring down reporting dictionary

- European Central Bank (ECB) discovered that the Banks’ Integrated Reporting Dictionary (BIRD) website 15 August 2019 was breached
- breach was discovered after routine maintenance
- BIRD website provides the banking industry with details on how to produce statistical and supervisory reports

- Possibly the contact data (but not the passwords) of 481 subscribers to the BIRD newsletter may have been captured e.g., email addresses, names and position titles of the subscribers
- attacker may use this data for further activities (e.g., conduct spear phishing attacks to high rank officials, management staff)

Retefe: The 5 year long banking malware

- Retefe is a special banking malware that has been seen active between 2014 and 2019
- banking malware that is primarily targeting German, Swiss and Austrian individuals
- malware operators used advanced methods to redirect users to spoofed internet banking sites in order to steal banking credentials

➡
- malware evolved from using proxies to Tor network and stunnel (secure tunneling) to redirect users in spoofed sites to achieve its illicit purposes

Typical Retefe attack scenario:

- infected users are directed to fake HTTPS login pages, when trying to access their e-banking
- fake site requires login credentials and/or additional personal data
- unsuspecting victims can easily be fooled

DarkVishnya: Eight banks hacked in Eastern Europe

- at least 8 banks were hacked from the inside between 2017 and 2018
- executed with the use of inexpensive netbooks, Raspberry Pi and Bash Bunny
- didn’t use any of the traditional delivery methods like phishing emails but a visitor pretending to be a courier or a job seeker connected the device to the banks’ network
- device offers remote access to the attackers via e.g. a 3G/LTE (Long Term Evolution) modem
- difficult to detect because there is no infection in the banks IT equipment

Cobalt Group Cybergang

- cybergang targeting financial institutions (e-payment systems, ATMs, SWIFT)
- cobalt is likely associated with the Carbanak remote backdoor
- e.g., :
  - SpicyOmelette attacks: vulnerability in a JavaScript script to grant attackers remote access to infected systems.
  - Infection of the systems delivered via phishing emails
  - Once the victim clicks on them he/she is redirected to an Amazon Web Services (AWS) Uniform Resource Locator (URL) controlled by Cobalt
  - installs the SpicyOmelette script, which appears signed by a valid and trusted certificate authority (CA)

- banks in more than 40 countries have been allegedly attacked by Cobalt group: losses are estimated to be above EUR 1 billion

Europe Physical Security Attacks: ATM Robbery on a BNP machine in Nanterre

- BNP ATM machine in Nanterre 2017
- officer in charge of resupplying an ATM was beaten to the ground and handcuffed and threatened with a gun by several individuals disguised as police officers
- Forced to open the airlock, and enter the codes allowing the money to be recovered

→

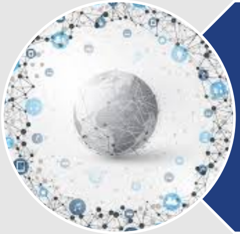
- robbery of 400,000 euros

Other Incidents

- BNP ATM machine in Nanterre 2017
- officer in charge of resupplying an ATM was beaten to the ground and handcuffed and threatened with a gun by several individuals disguised as police officers
- Forced to open the airlock, and enter the codes allowing the money to be recovered

➡

- robbery of 400,000 euros



Lessons Learned

Cyber Security Incidents & Lessons Learned

Incident	Lessons Learned
Bangladesh Bank cyber heist	• SWIFT transactions should be conducted only on computers that are isolated from the rest of the network • special security measures should be employed for every computing system that accesses the SWIFT computing system
Dridex take down operation and revival	• collaboration among financial services firm around the world • sharing information information with security experts & law enforcement agencies, enable the disruption of cybercrime teams
Attack against the Bank of Valletta	• risk assessment to account the vulnerabilities of multiple assets, interdependencies and cascading effects of possible attacks • need for becoming more proactive

Cyber Security Incidents & Lessons Learned

Incident	Lessons Learned
ECB bring down reporting dictionary	• isolation reduces the potential cascading impacts on other more critical systems
Retefe: The 5 year long banking malware	• users won’t verify the certificate issuer → vulnerable to data and money theft • banks must therefore make sure that their users become aware of such attacks

Cyber Security Incidents & Lessons Learned

Incident	Lessons Learned
Cobalt Group Cybergang	• need for integrated risk assessments that cover all assets • importance of building and disseminating cyber-security knowledge that is specific to financial sector
DarkVishnya: Eight banks hacked in Eastern Europe	• several attacks are launched from the inside • importance of inside security measures such as the verification and use of trusted devices
ATM Robbery on a BNP machine in Nanterre	• physical security attacks against the banking system are still happening • technology (e.g., surveillance systems) can boost protection against such incidents

Extending the Lessons Learned for the Finance Sector

- Increased use of e-transactions today: more opportunities for cybercriminals

- Organized cybercrime gangs difficult to dismantle: developed malware re-used by new cybergangs
  → catching the criminals is not the solution, their approaches evolve

- Law enforcement operations need international cooperation: cybergangs are set up worldwide & rely on remote hacked infrastructure for their activities
  → implementation of automated and trusted data exchanged

- Cybercriminals utilize different techniques to evade detection

- Malicious parties evolve their approaches in accordance to current IT trends
  → financial institutions must remain at the forefront of security innovation