Largest Bank Heist

That you probably don’t know about.

@iBotPeaches

sourcetoad

Story Time

- Greatest Bank Heist Ever
- Bangladesh (2016)
- Lets break down the events

May 2015 (Philippines)

- 4 new accounts opened, minimum $500
- Nothing suspicious.
- Accounts left untouched for months

January 2016 (Bangladesh)

- Employee opens an email
- Word document infected with Dridex

January 2016 (Bangladesh) - Part 2

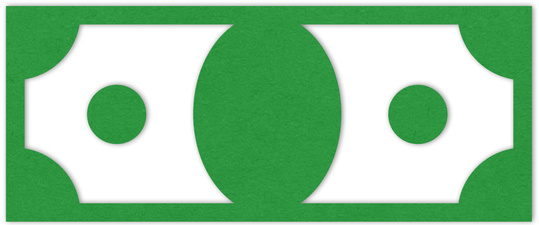
- Access to Bank is granted to hackers
- Hackers learning how Bank works
- Clock is counting down till the hack

February 4, 2016 (Thu - Bangladesh)

- End of Day, office closes.
- 35 transactions totaling 951 million dollars requested via SWIFT network
- Office closed - Fri/Sat

February 5, 2016 (Fri - New York)

- Bangladesh has a large account at Federal Reserves in NY
- The request was to move money across Asia to various entities
- No direct communication line to Bangladesh.



February 5, 2016 (Fri - New York) - Part 2

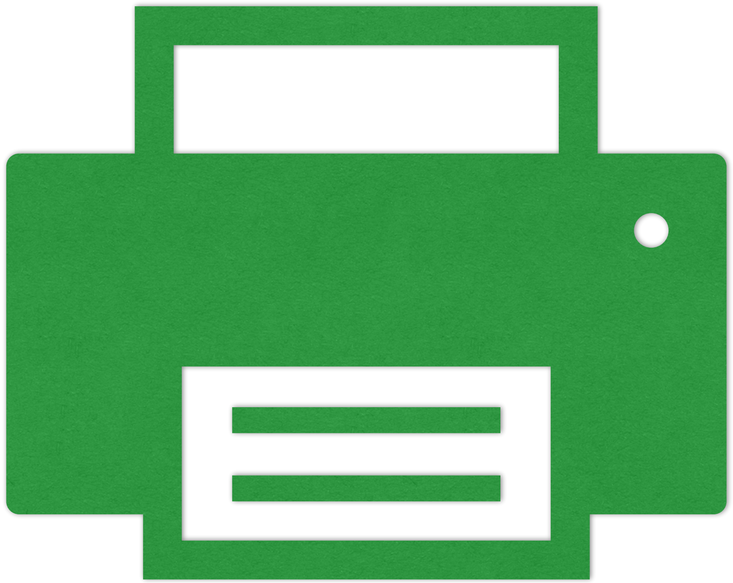
- First batch (35) denied, 2nd batch arrives
- SWIFT Orders processed, but awaiting review before released
- International banks move money a lot, so not out of the ordinary

February 5, 2016 (Fri - New York) - Part 3

- 2nd batch - 30/35 transactions blocked
- Name of “Jupiter” was flagged due to political International mess
- 5 transactions in progress

February 6, 2016 (Sat - Bangladesh)

- Printer isn’t working. Can’t see orders
- Small Saturday staff reports problem and waits for Sunday (work day)



February 7, 2016 (Sun - Bangladesh)

- Staff takes hours and discovers 35 transactions and panics
- New York is closed. No direct contact
- Sending STOP orders to every bank

February 8, 2016 (Mon - Sri Lanka)

- 20 million shows up via Deutsche bank
- Employee is surprised about 20 mil
- Asks Deutsche Bank to confirm, due to non-profit company
- Hackers spelled Foundation - Fundation
- **Transaction Reversed**

February 8, 2016 (Mon - Bangladesh)

- Recovered 31/35 transactions.
- Final 4 at same bank - RCBC in Manilla
- Unable to reach bank with STOP orders
- Multiple banks aware now

February 8, 2016 (Mon - Philippines)

- Chinese New Year
- Bank Closed
- 4 transactions, 81mil
- 4 accounts
- Each account funded with a transaction
- Withdrawals happening quickly

February 9, 2016 (Tue - Philippines)

- Bank gets STOP orders.
- Too late. 51.85 million already gone.
- Seems fishy, but local law.
- Money converted to local currency, moved to casinos to hide path

February 2016 (Tue - Philippines)

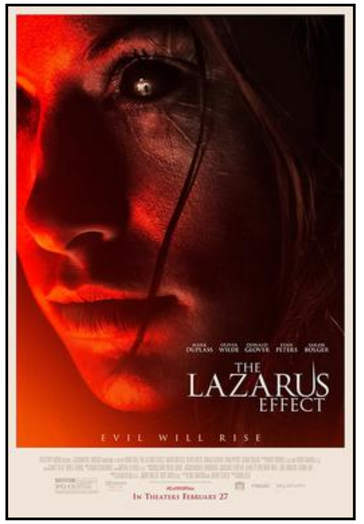
- Won’t freeze accounts till criminal case.
- Accounts moving money still!
- Accounts frozen when combined total is 65k left.

Success. 80.45 million stolen

- Money laundered, ends up in Macau
- North Korea “outside” point of financials
- World wide investigation

Hacker Group Identified - Lazarus

- Also known as - Hidden Cobra
- DDOS Attacks, Sony hacks, Crypto hacks
- Investigations think North Korea based
- Disabled Printer



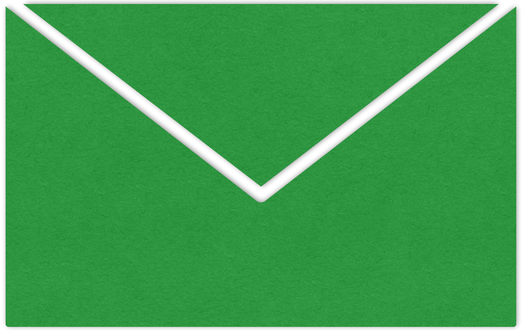
sourcetoad

Cold Cases Broken.

- Similar worldwide SWIFT transactions matching this hack
- Security upgraded worldwide

International Implications

- North Korea involved.
- State sponsored? Rogue?
- Blackmail? International help?
- What happened in Manilla?



RCBC Manilla

- Ignored STOP Order, for fear of life (?)
- Fake names opened up accounts
- Forged signature
- Dirty staff
- Local Law - Criminal case

In Closing

- Close times abused
- Timezones abused
- Local laws abused
- Months of planning (possibly more)
- Relatively unknown hackers

Connor Tumbleson
Senior Software Engineer
@iBotPeaches / connortumbleson.com

sourcetoad