Attacks on the global financial network SWIFT: A case analysis and Detection of Payment Fraud

EastNets
en.abling confidentiality

ISFS
INFORMATION SECURITY CONFERENCE FOR THE FINANCIAL SECTOR
QATAR CENTRAL BANK

Global Readiness

Hiscox Cyber Readiness Report 2017

EastNets
en.abling confidentiality

The incidence of cyber-attack is high.

- 57% Experienced an attack in the past year
- 42% have to deal with two or more

The average cost of the largest cyber security incident experienced ranges from

- €22,000 for very small companies
- US$102,000 for very large US companies

Business as usual? Not so fast

- 37% took them two days or more to discover the problem
- 46% took them two days or more to get the business back to normal

Some Known Incidents

- Central bank of Bangladesh (81 M$)
- Turkey's Akbank (4 M$)
- Banco del Austro (12 M$)
- Russia's Central Bank (31 M$)
- Reports of multiple Banks being hit by similar attacks —especially in Latin America theft upwards of US$10M per bank

Some Known Incidents

- A Vietnamese bank, Tien Phong Commercial Joint Stock Bank, blocked an attempt to transfer $1.36 million from its accounts in late 2015.

- July 2016, breach of one of Union Bank of India nostro accounts had been quickly detected and that attackers' attempts to fraudulently transfer funds from that account had been foiled.

Payments Fraud: Bangladesh Case

EastNets
en.abling confidentiality

2015

May – 2015

- 4 Fake accounts opened at RCBC Bank Manila
- Apparently with fake documents/ signatures

Oct – 2015

- Bank Bangladesh (BB) live with major tech upgrade and enables STP/RTGS

Jan – 2016

- Hackers target BB & send emails with malware attachments
- Malware harvests intelligence, on BB cash payment policy and procedure, transfer order protocol

Feb – 2016

With stolen credentials, on a BB holiday 4 and 5 Feb

- Hackers generate payment orders using SWIFT to NY Fed
- 35 SWIFT transfers (US$951m) to Sri Lanka/Philippines
- Fed did not process 30 transfers, they did 5 (US$101m)
- 1-Sri Lankan NGO (US$20m), blocked-recipient spelling error
- 4-RCBC Philippines (US$81m) went through

US$81m laundered within Philippines

- Deposited, routed via personal & money remittance company accts
- Subsequently to no. of casino accts in Philippines
- Breached printer at BB-previous day transactions could not be printed and reconciled
- During this time-RCBC branch Security Cameras were out of order

Payments Fraud: Bangladesh Case

EastNets
en.abling confidentiality

BB noticed discrepancy

- Routing bank query (Deutsche Bank) prompted BB
- Recognized on Sat, could not reach Fed during US weekend
- To complicate things, Mon/Feb 8 – Chinese New Year in Philippines
- Typically high value transactions to casino's went unnoticed/ common
- Per regulations, dollar remittance entering Philippines, has to pass through correspondent banks in US
- In this case, Citi, Wells Fargo, Mellon etc.
- BB issues stop orders

11 Feb

- BB requests Philippines Central Bank for help

29 Feb 2016

- Philippines Court petitioned to freeze accounts at RCBC Bank
- Order issued on 1 March

Latest

- Reports of multiple Banks being hit by similar attacks –especially in Latin America theft upwards of US$10m per bank
- Laundering currently being investigated by Philippine senate
- Two Chinese nationals in the gambling business in Macau and Philippines are being interrogated
- Investigators have identified 12 Philippine and 8 Sri Lankans nationals

Possibilities

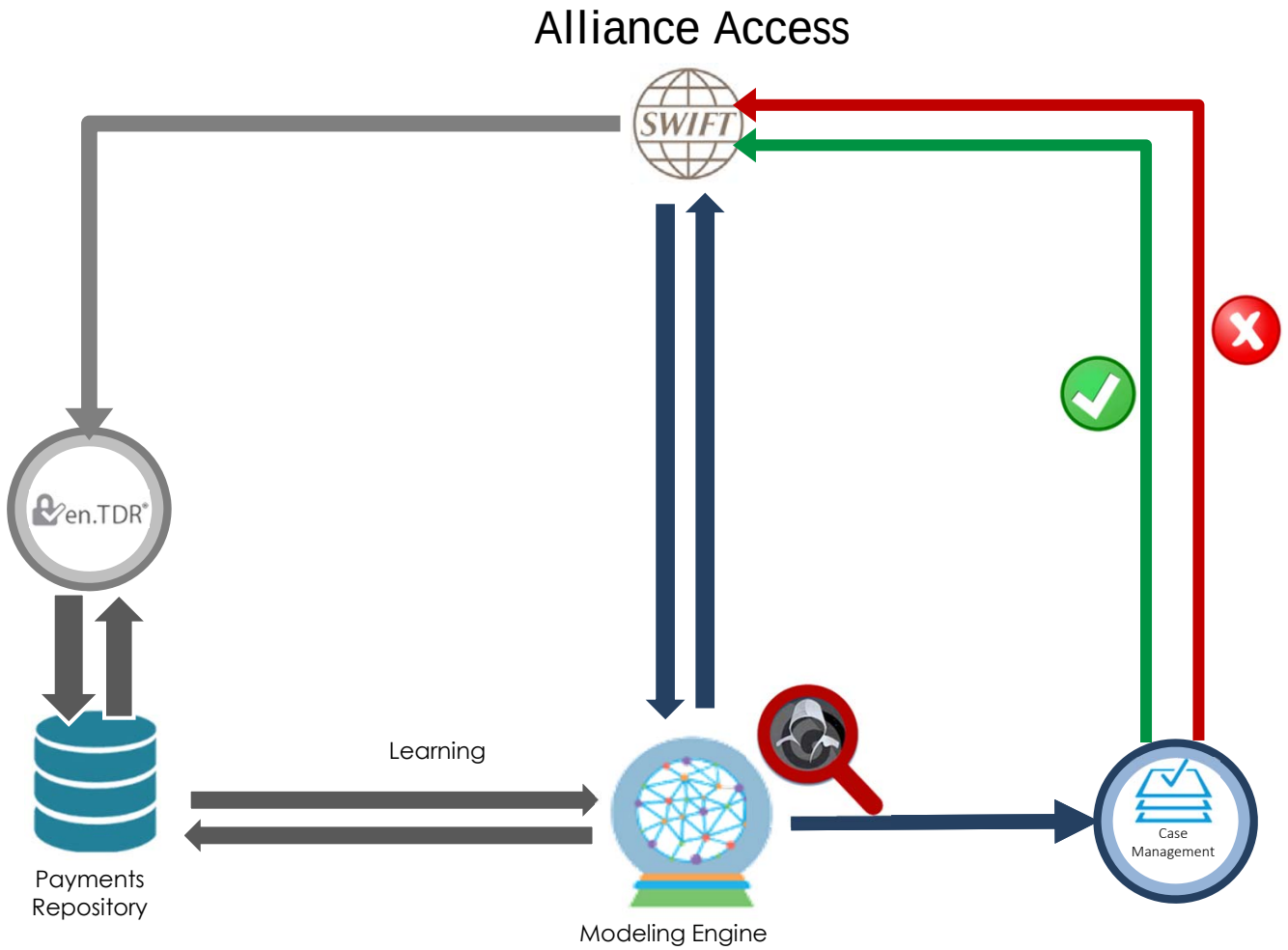
- Malware to provide attackers with environment details and access details.
- Creation of MT messages by unauthorized access to SAW.
- Injection of MT message files to message partners (files or queues).
- Payments created in back office by unauthorized users.
- Bypassing checks and validations during routing.
- Internal Fraud
- E-banking

Lines of Defense

EastNets
en.abling confidentiality

NOT ENOUGH ?

en.SafeWatch PaymentGuard



How we model Fraud

- BIC and User Profiling and Activity Monitoring
- Correspondent Profiling and Activity Monitoring
- Reconciliation of Statements
- Source Verification
- Bank, Unit, User, Correspondent business hours monitoring
- NACKs Monitoring
- Manual Activity/intervention Monitoring
- Anomaly messages that do not follow any usual pattern.
- Consistency & Duplicate messages.
- Thresholds, Countries, etc.

Warnings

Warnings are events and notifications not causing messages to be stopped

- Manipulated messages
- Deleted Messages
- Messages bypass the PG queues
- Login of users after usual working hours
- Any en.TDR WatchDog event
- Database inconsistency
- Routing schema changed
- ADK Component stopped

Fraud Cases Covred by PaymentGuard

EastNets
en.abling confidentiality

Originating from SAA

Originating from Back Office

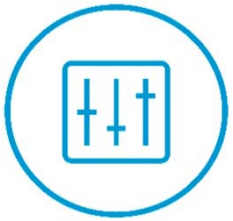
Originating from e-Banking

Other Security Aspects

EastNets
en.abling confidentiality

Two factor authentication

All Communications links are secured by SSL



Detected Messages are Reserved

Data In the DB is protected from Manipulations

PG Components are monitored

EastNets®

en.abling confidentiality

1000+

customers globally

13

Regional Offices

250+

FIs connected on ENSB

30+

years in operation

19

Global Channel partners present in 30 countries

EastNets
en.abling confidentiality

- WWW.EASTNETS.COM
- INFO@EASTNETS.COM

THANK YOU