STP house Message$hield: protect your SWIFT infrastructures

All secured banks are alike; each unsecured bank is unsecured in its own way…

The fairytale of payment hacking

Once upon a time, far up in the mountains, there was a little kingdom. It was rich, peaceful and green all year long. But the people of Beautyland never saw it coming.

The evil ruler of the neighbor kingdom Darkland was building a huge army and was planning funding it by stealing Beautyland's money. Darkland's agents built a secrete cyber platform. It was very powerful and sophisticated and penetrated the underlying banking infrastructures of Beautyland. It generated secrete, undetectable money transfer orders, funding Darkland's growing army. The plan was carefully executed and went on for months.

The legend also tells us the theft was detected only after millions were stolen. Until today no one knows if money was stolen from other countries too, but Darkland's army is still growing…

The real story about SWIFT payment hacking

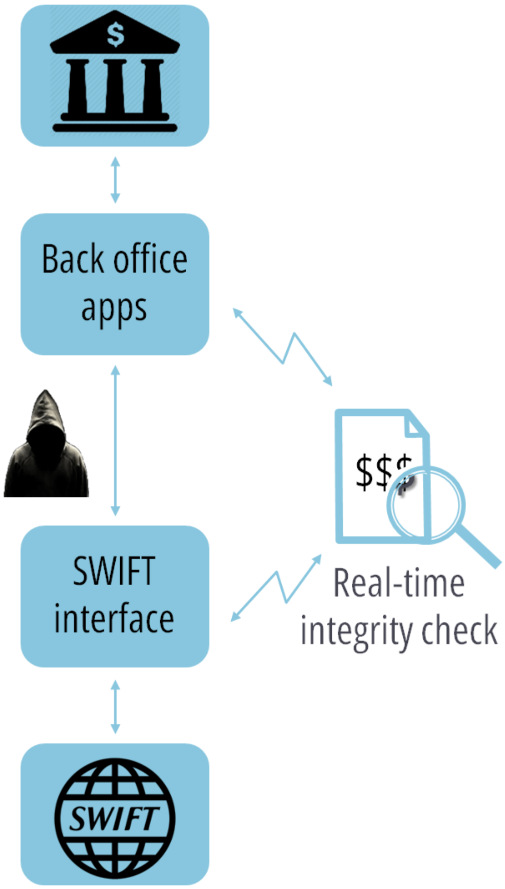
On Feb 2016, Bangladesh central bank announced its SWIFT infrastructures were compromised and 101 m Euro were gone. This event was the turning point of a global acknowledgement and appreciation of the immediate threat of cybercrimes over the global payment platform. More reports and attack findings from around the globe strengthen the understanding the banking industry is exposed.

As a result, SWIFT enhanced their security measures and recently published a mandatory policy and guidelines, called SWIFT Customer Security Program (CSP). SWIFT's CSP serves as global standardization and foundation for security protection, to be immediately adopted by the whole SWIFT community. Each bank should analyze, define and implement processes, tools and measures to prevent SWIFT network from fraud or unauthorized payment transactions.

STP house Message$hield – Anti hacking tool

STP house helps your bank to adopt most efficient measures and safeguard your SWIFT environment! We introduce a robust, lean and effective protection layer for your SWIFT traffic. Our solution prevents hackers from sending messages via SWIFT interface "under the radar" or changing the content of legitimate messages generated by the back-office throughout its messaging flow.

STP house **Message$hield** identifies at real time any unauthorized transaction and verify the integrity of every message before it is sent out to SWIFT. The solution is performance driven and brings immediate value to our customers.



Characteristics of an effective hacking prevention tool

To protect your payment infrastructure and prevent hackers from sending fraud transactions, there are several critical elements and implementation considerations. Our **Message$hield** addresses them all:

- **Real time** – our solution verifies the integrity of any payment messages at real time, before it goes "out the door". Any exception is immediately reported and alerted via SNMP interface.
- **Integrity check** of the actual SWIFT outgoing traffic vs the back-office traffic, assuring the traffic was not compromised.
- **Shortening investigation process** – by allowing top down investigation approach and complete traceability.
- **Complimentary to SWIFT CSP** – our solution is designed and built in accordance with SWIFT's regulation to shield the bank from cyber risks.
- **Fast and easy implementation** – the solution is ready out of the box, requiring very short implementation and fast adaptation to the relevant back office applications and to SWIFT interfaces (SAA/AMH).

For more information about STP house's **Message$hield** and the benefits it can bring to your organization, please contact our SWIFT Security Advisory experts, at cyberexpert@stphouse.com