SWIFT ISAC Report
April 2019

Three years on from Bangladesh

Tackling the adversaries

Introduction

In February 2016, Bangladesh Bank famously became the victim of a cyber attack targeting the bank's infrastructure connected to SWIFT. Rapidly following the attack SWIFT launched its Customer Security Programme in a concerted effort to drive industry-wide collaboration against the cyber threat and to help reinforce and safeguard the security of the wider ecosystem.

Relevant and timely intelligence is a critical factor in effectively defending against cyber threats. This is why we established a dedicated Customer Security Intelligence (CSI) team to investigate customer incidents and share back anonymised information with the community. Focused on customer security forensics and analysis, the CSI team undertakes investigations of potential threats and customer security incidents and shares the resulting information with the community through the SWIFT ISAC information sharing portal.

Three years into the CSP, we have issued multiple updates on how the Modus Operandi, the tactics, techniques and procedures (TTP) have progressed, providing valuable insights into how cyber prevention and detection measures should evolve.

At the start of 2018, SWIFT set out to increase its collaboration with industry experts, including anti-virus vendors and incident response teams. The efforts rapidly paid off as the closer collaboration resulted in the quick identification of financial institutions targeted by cyber criminals – in most cases before fraudulent transactions were even sent.

Most of these attacks have been identified (and stopped) in the preparation phase. However, in a subset of the attempted attacks, fraudulent cross-border payment instructions were issued by the attackers. Even then, however, many of these fraudulent instructions were later stopped thanks to the intervention of banks along the payment chain.

This evidences how, whilst fraud and cyber detection measures are first and foremost sender responsibilities, financial institutions involved within the payment flow can also play important roles in identifying and detecting fraud – roles that become increasingly important as the speed of cash pay-outs increases, as it is doing. Indeed, while the timing in the Bangladesh Bank case involved several non-working days between the attack and final pay-outs, in recent cases the cash pay-outs have taken place within a matter of hours.

In this report we examine the trends we observed over the course of 2018 and 2019, showcasing how both business and security information can utilise tell-tale signs, and become key in detecting and responding to attempted attacks.

Notwithstanding the increased success level in detecting and preventing attacks, it is critically important for industry participants and their security partners to understand how the attackers have evolved – and how quickly they can adapt their attack patterns to avoid detection. This report, together with the technical detail published on the SWIFT ISAC portal, aims to help customers in this endeavour.

The main characteristics set out in this report relate to the evolution in the location of Target banks, in the amounts attempted per fraudulent transaction and in attackers' reconnaissance practices and timing. The report also describes how attackers are varying their practices as far as timing, and preferred currencies are concerned, and it identifies the regional locations of the compromised or "mule" accounts used in these attempted thefts.

Relevant and timely intelligence is a critical factor in effectively defending against cyber threats.

Targets

SWIFT has engaged closely with industry experts such as anti-virus vendors and incident response teams. This collaboration, which intensified considerably over 2018, has helped contribute toward the proactive identification of financial institutions targeted by cyber criminals.

In the majority of these cases, the attacks have still been in the reconnaissance phase; user workstations had been compromised but the attackers had not yet been able to access banks' payment systems.

While SWIFT does not reveal the names of the financial institutions that have been targeted in cyber attacks, SWIFT is able to disclose anonymised information related to them that can be used preventatively by others – such as the common characteristics shared by typical Target institutions.

In most cases, the Target banks have been located in countries with a (very) high risk rating on the Basel AML Country Corruption List[1]. Over the course of the last fifteen months, the majority of the attacks targeted financial institutions in Africa, Central Asia, South East Asia and Latin America.

In all cases the Target institutions were smaller banks in terms of cross-border transactions per day.

As well as ensuring that environments are protected from a technical point of view, all financial institutions should be able to detect fraudulent transactions and should be ready to respond at a business level if they find they are victims of attacks. All SWIFT customers need to acquaint themselves fully with the payment cancellation process and messages, as well as the **gpi Stop and Recall facility**.

In the vast majority of cases investigated, fraudulent transactions were inserted using the interface GUI. This means that the instructions would not have been present in payment back office applications and, as such, would therefore have been detectable through verification of end-of-day / start-of-day statement reconciliation messages which are typically sent by Nostro Account owners. These messages contain overviews of the activities on the Nostro Account on the given day.

Additionally, financial institutions can opt to use SWIFT's **Daily Validation Report** tool to detect the usage of new corridors and/or large deviations in existing corridors and SWIFT's **Payment Controls Service**, which enables financial institutions to ensure that particular combinations of amounts, currencies, corridors or countries require out-of-band confirmation. Whilst the Payment Controls Service only recently launched, end-of-day reconciliation based on the Daily Validation Report tool has already proved invaluable in helping customers detect attempted frauds and thus prevent potential losses.

Amounts

Over the last three years, customers' anti-fraud systems and other anomaly detection systems have helped thwart the attackers in many instances. Fine-tuning these systems is imperative to their success.

Sending fraudulent high value payment instructions can lead to large rewards, but the higher the value of the instruction, the higher the risk of triggering fraud detection systems. Since the cyber incident in Bangladesh, the amounts sent in individual fraudulent transactions has evolved, making them harder to detect. Up until early 2018, we typically saw per transaction amounts of ten or tens of millions USD, however since then attackers have significantly reduced average per transaction amounts to between 0.25 MUSD and 2 MUSD – presumably to help avoid detection.

As noted earlier, fraudulent transactions were typically issued using new "payment corridors"[2]. In the cases where existing corridors were used, we noticed large deviations in value. Typically, we saw that per transaction amounts sent on existing corridors were much larger than the 'average' amounts sent over them in the prior 24 months. Targeted banks can identify such anomalies using the **Daily Validation Report** tool, while Receiver banks and Beneficiary banks can implement similar algorithms to identify suspicious behaviour based on historical traffic patterns.

In each such attack we investigated, most of the transactions issued were handled by one or two Receiver banks and were intended for the same Beneficiary country. During the most recent investigations, the number of fraudulent transactions issued averaged around ten per incident within a two-hour period.

Sender banks are able to identify, flag and investigate such increases in traffic using the **Daily Validation Report** tool, while Receiver and Beneficiary banks can implement detection techniques based on sudden increases in messages using particular corridors, or particular combinations of sending banks and Beneficiary countries.

Customers' anti-fraud systems and other anomaly detection systems have helped thwart the attackers in many instances.

[1] Basel AML country risk profile

[2] A payment corridor refers to a sequence of banks in a payment chain – i.e. the Target/sending bank, the Receiver bank/Nostro Account owner and the Beneficiary bank.

Reconnaissance

Enticed by the prospect of potentially lucrative pay-outs, attackers are persistent; they will often penetrate a target and wait for weeks or even months before launching an attack, using the time to learn patterns and behaviours and plot their fraud. Whilst they will operate "silently" during this reconnaissance time, it is a critical period during which they can be detected.

The initial response to a detected intruder is vitally important – even if there is no evidence of visible theft or attempted theft.

Without a cyber security incident response plan in place, it is near impossible to ensure an adequate initial response. An inadequate response can lead to the loss of valuable investigative information, and the subsequent inability to determine the full scope of the breach (e.g. an exhaustive listing of all compromised hosts and user credentials, all data exfiltrated, and any malware deployed).

Furthermore, for as long as actors haven't been fully eradicated from compromised environments, they remain a risk. Once they become aware that they have been discovered they can either rapidly change tactics or choose to remain dormant for a while before renewing their attack when the Target is enjoying a false sense of security.

SWIFT Customer Security Controls Framework

The security of our community requires everyone's participation and starts with each individual organisation's own security. To help with this, in March 2017 SWIFT published the Customer Security Controls Framework (CSCF).

The CSCF is a set of security controls – both mandatory and advisory – that set a security baseline for all SWIFT users.

The controls were developed in conjunction with industry experts and designed to be in line with existing information security industry standards: PCI-DSS, ISO 27002, and NIST. Attesting compliance with the controls is an essential step for customers towards securing their SWIFT-related infrastructure.

As part of the Change Management process for the CSCF, control updates are usually announced mid-year, with attestation and compliance against the mandatory controls of any new version required between July and December the following year. This is intended to allow sufficient time, up to 18 months, for customers to budget, plan and implement any required updates.

Timing

Timing is everything – including in determining the success of a cyber attack. The following graphic illustrates the role that timing has to play, showing the local times at which fraudulent transactions were sent.

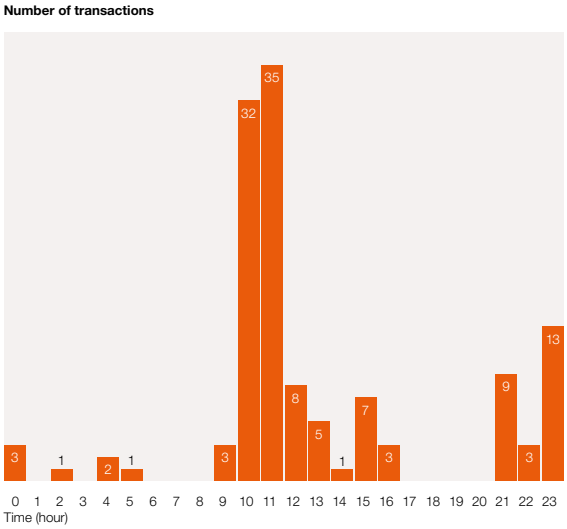
Two main patterns can be identified:

1. Attackers try to send messages outside business hours or during public holidays in order to avoid detection by the Target institution; or
2. Attackers try to send messages during business hours to blend in with legitimate traffic of the Target institution to avoid detection by the counterparty and Beneficiary institutions.

Fraudulent messages that go undetected for a longer period of time have a higher chance of reaching Beneficiary accounts, and as such have a higher chance of being cashed out. Responding in a timely manner to cyber security incidents and having structured and tested reconciliation and cancellation processes in place can help reduce the financial impact of a cyber security incident.

The attack on Bangladesh Bank took place the evening prior to a series of non-working days in the different countries involved in the payment flows.

In more recent incidents, however, the attackers started to issue fraudulent payments during working hours on business days. Furthermore, the cash-outs in recent incidents have taken place within a matter of hours.



Message Types

Based on the cases we have observed over the last 15 months, the attackers' message type of choice in cross-border fraud is typically the 'Single Customer Credit Transfer' or MT103[3] message type. Apart from a few isolated cases, all of the fraudulent transactions issued during customer cyber incidents known to SWIFT involved MT103 messages[4].

Another notable coincidence is that all of the messages were processed by at least three different financial institutions in three different countries:

1. The Target bank ("Sender BIC" or "Sender")
2. The Receiving bank or Nostro Account owner of the Target bank ("Receiver BIC" or "Receiver")
3. The Beneficiary bank ("Beneficiary" or "Account With institution")

All three banks have roles to play in the identification of fraudulent transactions. In SWIFT terms, we call the combination of these three banks the "payment corridor".

The vast majority of the fraudulent transactions we investigated over the last 12 months used corridors that had not been used in the previous 24 months. This is particularly interesting for Target banks who can filter outgoing transactions using SWIFT's **Payment Controls Service** to specify which corridors they use on regular basis, whilst requiring additional confirmation on other corridors.

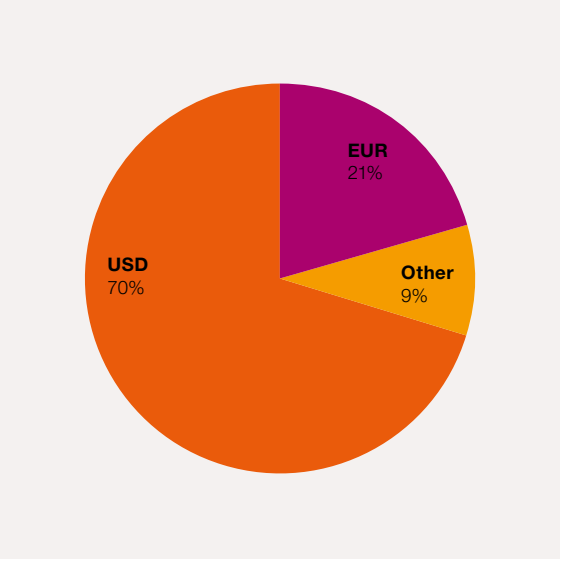
Targeted banks can also identify, flag and follow up on new corridors using SWIFT's **Daily Validation Report** tool, while Nostro Account owners can play an important role by identifying, flagging or querying payments along new corridors.

Currencies

With the USD accounting for the majority of cross-border traffic, it is no surprise that it was the currency used in the majority of incidents investigated. Overall, the USD accounted for approximately 70% of the fraudulent messages created since the 2016 attack.

Since the incident in Bangladesh Bank in 2016, however, we have also observed an increased usage of European currencies – most notably EUR and GBP, while a small minority of incidents (approximately 5%) involved Asia Pacific currencies – mainly HKD, AUD and JPY. This evidences the importance of Receiving Banks paying attention to their customers' usage of all these international Nostro Accounts, not only USD accounts.

The below graph shows the currencies used in fraudulent transactions since 2016.



[3] MT 103 Single Customer Credit Transfer

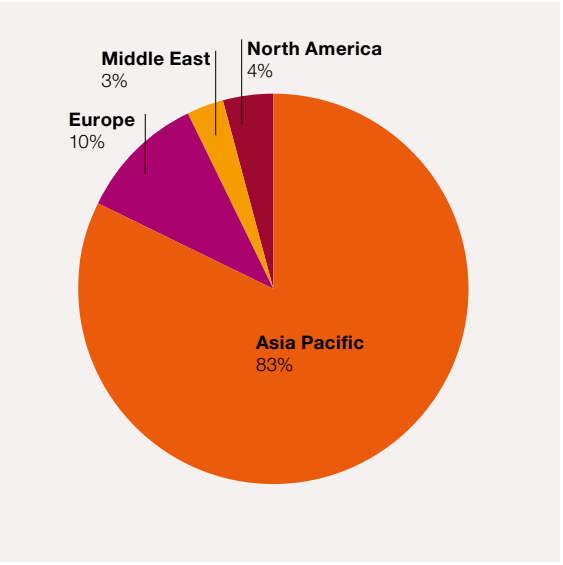
[4] SWIFT observed the usage of an MT102 in one isolated case and the usage of MT202COV in a few cases, covering fraudulent MT103s.

Beneficiaries

Beneficiary or "mule" accounts are critical for attackers' ability to extract funds from the financial system – without these compromised accounts they would be unable to materialise any of the fraudulent funds. Gaining an understanding about the profile of these accounts can be equally valuable to those fighting against the frauds.

The small subset of investigated cases in which the adversaries managed to initiate fraudulent message instructions provides interesting data on the Beneficiary accounts. SWIFT was able to extract Beneficiary country information from the fraudulent messages sent in 2018 – information which revealed some differences in pay-out techniques. What was most notable, however, was the concentration of the Beneficiary banks in Asia Pacific: 83% of all fraudulent transactions had a beneficiary account in South East Asia. The remaining 17% was spread over other regions including, in order of magnitude, Europe, North America and the Middle East.

The below graph illustrates the regional location of Beneficiary accounts used in fraudulent transactions since July 2018.



The Payment Controls Service enables banks to implement more effective and robust controls.

Strengthen your defences

The Daily Validation Report tool and Payment Controls Service are part of SWIFT's financial crime compliance portfolio and an important element in the CSP to strengthen the global financial community's defences against cyber threats as the frequency and speed of payments increases.

Daily Validation Report

The Daily Validation Report tool helps to mitigate the risk of lost records by providing daily activity and risk reporting of your previous day's SWIFT transactions. Activity reporting allows institutions to verify their payment message activity against SWIFT's own record – which is critical if customer environments are compromised. Risk reporting allows institutions to focus on changes in activity that may indicate significant payment risks, provides aggregated transaction totals by counterparty, and flags new correspondent relationships.

Each day's report covers the previous day's payment activities for MT 103, MT 202, MT 202COV, MT 205 and MT 205COV message types. Reports are delivered via a completely separate, secure online channel, direct to compliance and operations teams for monitoring.

Payment Controls Service

The Payment Controls Service enables customers to screen payment instructions safely, before transmission, to detect any illicit or unusual message flows.

Using the tool, customers can define their own monitoring policy, controlling their parameters to enable timely detection and prevention of out-of-policy or uncharacteristic and therefore potentially high-risk transfer requests.

By understanding the patterns of payments sent over time, the Payment Controls Service enables banks to implement more effective and robust controls. Monitoring rules can also be deployed in real-time to enforce policies and protect payment operations. Doing this reduces the risk of fraud and gives operations teams tighter overall control.

Cyber Security Counterparty Risk Management

In order for customers to attest their level of compliance against the mandatory and advisory controls, SWIFT provides the 'Know Your Customer – Security Attestation' tool as the central application for the submission of self-attestation data. The KYC-SA application also enables each customer to facilitate the transparent exchange of their security status information with their counterparties to support cyber risk management and business due diligence.

The transparency provided by this counterparty data exchange system is driving attestation and compliance with the controls, as institutions seek to demonstrate their cyber security to their counterparties.

Cyber security risk introduced by counterparties needs to be managed alongside other types of risk. Many institutions are therefore already integrating cyber risk assessments into their existing risk processes by incorporating the assessment of counterparties' CSCF attestation data into their risk management and business decision-making processes.

As outlined in the recently published guideline "Assessing Cyber Security Counterparty Risk – A Getting Started Guide", institutions can assess the cyber security risk posed by their counterparties, by:

- Collecting the necessary data and correlating known incidents to support risk-driven decisions;
- Processing this data and transforming it into a weighted, risk-based assessment, typically shown as a numeric score or a red-amber-green indicator;
- Adopting suitable countermeasures to mitigate or 'treat' the risks;

To support the risk assessment of incoming transactions from counterparties, institutions should assess how incoming transactions from counterparties correlate against the profile of existing incidents, e.g: country/region of sending counterparty; country/region of end Beneficiary; Transaction type; transaction currency; transaction value; transaction timing and frequency.

These parameters are described in the Getting Started Guide and should be used by institutions to assess levels of counterparty risk.

Conclusion

The global financial community has seen a continued evolution in the cyber threat since 2016, with financial institutions facing attacks of increasing levels of sophistication.

In responding to this challenge, SWIFT will continue to promote robust cyber security standards, seek security-enhancing innovations in our own products and services, and work to increase the scope and quality of threat intelligence sharing.

Our information sharing initiative has contributed to significant improvements in the community's collective cyber defences as well as the introduction of fraud detection and prevention capabilities, such as the **Payment Controls Service** and the **Daily Validation Report** tool. These products are aimed at mitigating the risks associated with cyber fraud, and are designed to supplement the fraud controls that financial institutions should already have in place.

The industry should continuously increase the strength and diversity of its defences and ensure it understands the nature of the changing threat. This means being proactive in limiting criminal opportunities linked to systems and business practices, it means ensuring proper preparedness and understanding counterparty cyber risk.

Cyber security risk introduced by counterparties needs to be managed alongside other types of risk.

About SWIFT

SWIFT is a global member owned cooperative and the world's leading provider of secure financial messaging services.

We provide our community with a platform for messaging and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis and regulatory compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories. While SWIFT does not hold funds or manage accounts on behalf of customers, we enable our global community of users to communicate securely, exchanging standardised financial messages in a reliable way, thereby supporting global and local financial flows, as well as trade and commerce all around the world.

As their trusted provider, we relentlessly pursue operational excellence; we support our community in addressing cyber threats; and we continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Our products and services support our community's access and integration, business intelligence, reference data and financial crime compliance needs. SWIFT also brings the financial community together – at global, regional and local levels – to shape market practice, define standards and debate issues of mutual interest or concern.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's international office network ensures an active presence in all the major global financial centres.

For more information about SWIFT, visit **www.swift.com**.

57412 - April 2019