June 2016

Financial crimes observer

A publication of PwC's Financial Crimes Unit

SWIFT action: Preventing the next $100 million bank robbery

Attackers last February reportedly withdrew $101 million from the Bangladesh Central Bank by obtaining and exploiting the bank's credentials for the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network.[1] The attack – one of the biggest bank robberies in history – exploited weaknesses in cyber, fraud, and possibly insider threat controls, illustrating the need for banks to combine financial crime risk areas that were previously either siloed, or at best tenuously connected.

Specifically, the attackers exploited cyber weaknesses by designing custom malware tailored to bypass controls and network logging systems used by the Bangladesh Central Bank. The thieves also bypassed fraud controls by using the Bangladesh Central Bank's credentials to gain unauthorized access to the SWIFT network[2] and by setting up fraudulent bank accounts to receive and transfer the stolen funds. Finally, the attackers used detailed information about the Bangladesh Central Bank (including the brand of printer used by the bank) to commit the theft, suggesting that insiders may have been involved.

The attack is believed to be a part of a broader campaign targeting multiple banks, with banks in Vietnam and Ecuador experiencing similar incidents. Therefore, banks should be preparing for this type of attack and should become more vigilant for schemes targeting funds transfer systems. To do so, banks can focus on integrating (or better coordinating) their cybersecurity, anti-fraud, and insider threat management programs. This will provide a clearer view of the threat landscape, allow banks to better detect suspicious transactions, and help streamline investigations.

Additionally, banks should enhance their existing cyber, fraud, and insider threat controls to better detect and prevent similar attacks. First, banks should implement into their cyber controls a monitoring program for funds transfer systems, and review their cyber detection, prevention, and response practices to determine whether they are sufficient to counter similar attacks. Banks should also enhance their fraud programs by using behavioral analytics to detect suspicious activity and by more broadly applying customer due diligence policies. Finally, banks should mitigate insider threats by limiting the number of people with access to funds transfer systems to those who need to have such access.

This **Financial crimes observer** analyzes the Bangladesh Central Bank attack and provides our advice on what banks should be doing now.

Background on the attack

On February 4th, attackers used stolen credentials to send a series of payment instructions over the SWIFT network. The attackers initially sent 35 payment instructions totaling $951 million, but the Federal Reserve Bank of New York (New York Fed) only processed five of the payments, totaling $101 million.[3] The New York Fed did not process the remaining payments because it was unable to reconfirm the instructions with the Bangladesh Central Bank.

Of the $101 million reported to have been transferred, the thieves were able to successfully launder $81 million through casinos in the Philippines. The attackers attempted to divert the other $20 million to Sri Lanka, but the funds were recovered after the recipient bank in Sri Lanka flagged the funds transfer as suspicious.

Even though not all of the money made its way to the attackers' hands, the attack is one of the most successful bank robberies of all time. The success of this scheme is due to a combination of factors: exploiting weaknesses in cyber, fraud, and possibly insider threat controls; detailed knowledge of how banks interact with funds transfer systems; malware tailored for the specific target (and therefore not likely to be detected by broad-release anti-malware programs); and access not just to the funds transfer systems themselves but also to detection and response mechanisms. These factors combine to create a formidable threat that seems to be gaining momentum – effectively targeting entire business processes instead of individual systems.

Further details of the attack include:

- Malware was specifically tailored for the Bangladesh Central Bank, including functionality tailored to granular details, such as the brand of printer used by the bank – suggesting the possibility of inside involvement or extensive surveillance.
- The malware was custom-designed with the ability to bypass checks made by the software and systems used by the bank. This indicates that the attackers had intimate knowledge of such software and systems, including the interface to the SWIFT network and its database structure.
- The attackers manipulated network logging systems designed to detect the very activity that the attackers were performing.
- The attackers manipulated local printers, creating false confirmation messages to cover up the fraudulent transactions.
- The attackers activated dormant accounts to receive and transfer the funds.

What banks should be doing

Banks should begin preparing for this threat, and not wait until they are attacked. As an initial step, we recommend that banks investigate their current environment – beyond just traditional security log analysis – to determine whether they have already been attacked, or even just targeted, by this scheme.

Banks should also prepare for additional attacks as this scheme adapts and as additional attackers attempt to replicate its success. To do so, banks cannot rely upon standardized, automated cybersecurity systems alone. Rather, banks should integrate cyber, fraud, and insider threat management into a centralized program. Additionally, banks can apply lessons learned from the attack to enhance their cyber, fraud, and insider threat programs.

We recommend banks take the following steps:

Integrating financial crime areas

- Pool data from formerly-siloed areas of financial crime (e.g., cyber, fraud) into a central data repository. Using this data, identify red flags that could indicate suspicious transactions. Given the volume of transactions many banks will need to analyze, institutions should implement data analytic platforms to identify suspicious signals in a sea of transaction noise.[4]
- Conduct holistic financial crime risk assessments, which should:
  - Evaluate and prioritize threats based on historic, known, and emerging trends in financial crime – including the attack on Bangladesh Central Bank and similar attacks on funds transfer systems.
  - Estimate the severity and likelihood of attacks, and inventory existing mitigating factors.
  - Assess risks based on the existence of current controls, and recommend adjustments to controls and processes.
- Implement a cohesive financial crime case management system. Currently, many banks have several case management systems (i.e., central repositories for financial crime data) for various areas of financial crime (e.g., cyber, fraud). With multiple systems used to capture data, investigators often fail to realize that cases they are working on have linkages to incidents in other areas of financial crime. Banks that take a holistic approach to case management can respond more quickly to attacks, better prioritize investigations, and more efficiently distribute investigation workload. [5]

- Provide a central governance process for investigations, which should include clearly defined escalation paths and communication plans.

Cyber risk measures

- Conduct a thorough review of prevention, detection, and response practices to ensure they are sufficient to counter similar incidents. [6]
- Use intelligence from public reports, industry information-sharing, SWIFT, and threat intelligence services to identify the tactics and unique identifiers used in this attack (e.g., filenames, network communications structure) and use this information to scan for the presence of such identifiers within critical systems.
- Implement a system that monitors processes that interact with the SWIFT database and generates alerts when any new processes are detected.
- Monitor outbound traffic from critical systems (such as those systems that connect to SWIFT or other funds transfer systems) for anomalies.
- Confirm that the latest updates to SWIFT payments software (e.g., SWIFT Alliance Access, Alliance Entry) are installed.

Anti-fraud measures

- Implement behavioral analytics to identify and investigate suspicious behaviors, such as instances of repeated failed transactions.[7]
- Apply Know Your Customer (KYC) and Anti-Money Laundering (AML) policies retroactively to dormant accounts that suddenly show activity for large amounts in international or batch domestic transactions (especially to high-risk destinations such as casinos), and impose stronger validation and transaction-hold controls for high risk customers.[8]
- Review out-of-band validation controls (e.g., print-outs, email confirmations, voice confirmations) and understand how they can be manipulated (including by social engineering).[9]
- Develop a fraud typology specific to SWIFT and other payment transfer platforms, and assess fraud prevention and detection controls against this typology. Specifically, this typology should include:
  - Authentication rules
  - Transaction approval rules
  - Anti-fraud transaction surveillance
- Close or monitor gaps identified in the fraud risk assessment. Specifically, banks should focus on gaps in transaction approval and monitoring.[10]

Insider threat measures

- Identify who (e.g., employees, contractors, programmers, third party vendors) has authorized access to SWIFT or other funds transfer systems.
- Set a “need to have” policy on access to funds transfer systems, and limit the number of people with access to the minimum necessary by evaluating each user’s need and business justification against the “need to have” policy.
- Implement into funds transfer initiation policies and procedures a maker and checker requirement (i.e., a policy requiring that a separate employee authorizes a funds transfer than the employee that initiates the funds transfer), and require that the checker is of sufficient seniority to discourage internal collusion.
- Monitor for users who abuse or exceed their access. Implement an analytics program to identify anomalies in credentials or access to funds transfer systems (e.g., excessive logins, accessing the system at unusual times) and investigate red flags raised by the process.
- Expand background checks for all staff with access to funds transfer systems.
- Implement a “see something, say something” policy for employees and managers. Educate personnel about detecting this threat and reporting suspicious behavior, as well as escalation and whistleblower policies and procedures.

Endnotes

1. SWIFT is a network used by the financial sector to transfer funds. Most international funds transfers are made through the SWIFT network.
2. It is unclear how the attackers obtained Bangladesh Central Bank's credentials. PwC's *Financial crimes observer, Fraud: Email compromise on the rise* (February 2016) discusses various methods that attackers use to obtain credentials to access bank accounts and payment systems.
3. The New York Fed maintains accounts for approximately 250 foreign central banks (including the Bangladesh Central Bank) and provides payment services for such banks.
4. For additional information regarding data analytics, see PwC's *Financial crimes observer, Bank fraud: Old defenses won't stop new threats* (April 2016).
5. For more advice on implementing a cohesive case management system, see the *Financial crimes observer* cited in note 4.
6. For our recommendations on enhancing cybersecurity prevention, detection, and response practices, see PwC's *A closer look, Cyber: Think risk, not IT* (April 2015).
7. For additional information regarding behavioral analytics, see the *Financial crimes observer* cited in note 4.
8. For our recommendations on enhancing KYC and customer due diligence programs, see PwC's *Financial crimes observer, AML: Who is your customer? FinCEN wants you to know* (May 2016).
9. For additional information regarding the use of social engineering to bypass authentication controls, see the *Financial crimes observer* cited in note 2.
10. For additional information regarding fraud risk assessments, see the *Financial crimes observer* cited in note 4.

www.pwc.com/us/financialcrimes

Additional information

For additional information about this **Financial crimes observer** or PwC's Financial Crimes Unit, please contact:

Joseph Nocera
Cybersecurity Leader
+1 312 298 2745
joseph.nocera@pwc.com

Naoki Yamamoto
PwC Japan Cyber Security Leader
080-2105-3073
naoki.n.yamamoto@pwc.com

Sean King
PwC Japan Cyber Security Partner
080-4366-6596
sean.c.king@pwc.com

Joe Dubbs
PwC Japan Cyber Security Director
080-4061-7440
joseph.dubbs@pwc.com

Sean Joyce
Financial Crimes Unit Leader
+1 703 918 3528
sean.joyce@pwc.com

Simon Gealy
PwC Japan Financial Services Leader
080-3549-9530
simon.s.gealy@pwc.com

Michael Buxton
PwC Japan Risk Consulting Leader
090-9138-7630
michael.buxton@pwc.com

PwC Japan Group represents the member firms of the PwC global network in Japan and their subsidiaries (including PricewaterhouseCoopers Aarata LLC, PricewaterhouseCoopers Kyoto, PwC Consulting LLC, PwC Advisory LLC, PwC Tax Japan, PwC Legal Japan). Each firm of PwC Japan Group operates as an independent corporate entity and collaborates with each other in providing its clients with auditing and assurance, consulting, deal advisory, tax and legal services. At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC Network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.