KPMG

Cyber Watch - Threat Intelligence

Be in a defensible position.
Be cyber resilient.

Canadian Banks and financial organizations should heed warning issued after massive heist against Bangladesh Central Bank.

Recent developments reveal the massive heist against the Bangladesh Central Bank pose a much wider and very real threat to financial institutions, prompting a warning by SWIFT that banks should review their internal security in light of what has been uncovered. SWIFT, a global provider of secure financial messaging services, connects more than 11,000 institutions in over 200 countries and processed over six billion messages last year. In what can be described as an elaborate plan involving an apparent targeted malware attack on the bank to access SWIFT, the attackers put through requests for nearly US$1 billion, of which US$101 million was paid out, and US $81 million remains unrecovered. The latest discovery of this targeted malware has prompted warnings because it appears to be part of a larger attack toolkit. SWIFT may release additional updates as it learns more about the attack and other potential threats.

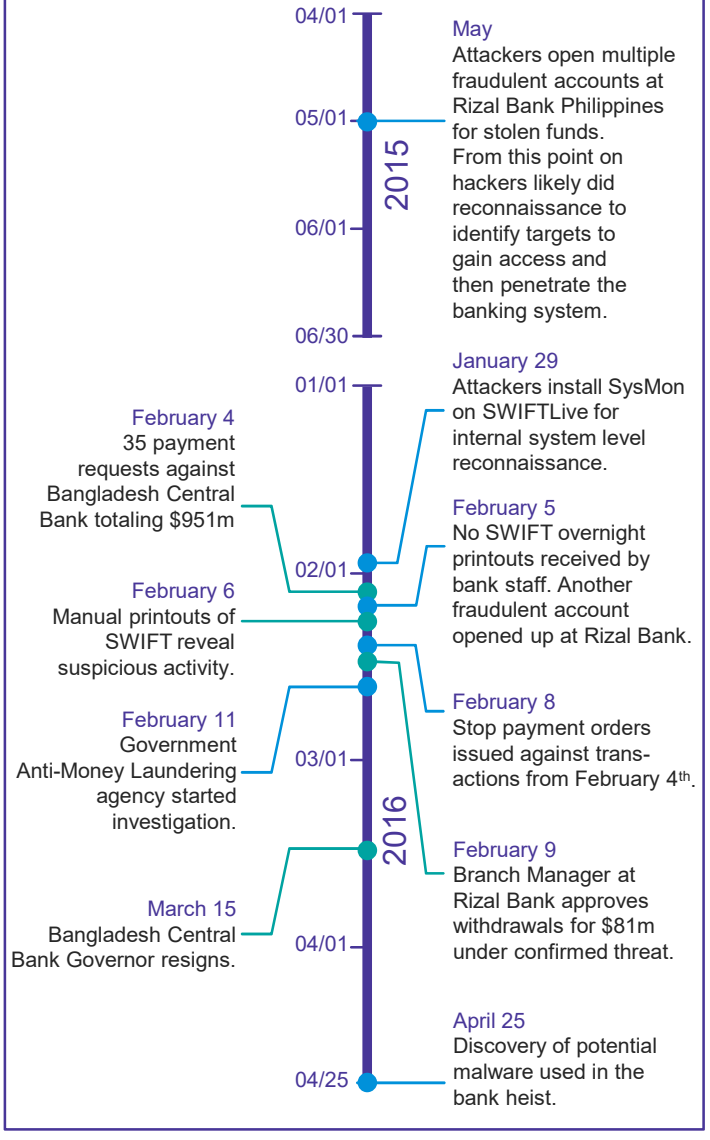
New developments.

Investigators have learned that fraudulent accounts to hold stolen funds had been set up in the Philippines in May 2015. There are indications the attackers were communicating with the network in late January. The operation itself took place February 4 and 5, when the targeted malware carried out its intended purpose, concealing the trail of 35 fraudulent payment requests, totaling $951 million. Fortunately for the bank, an error in a request stopped the bulk of the transactions; only five of the 35 were authorized and paid.

What should be noted is how the malware modified the SWIFT Alliance Access Server software to bypass authentication checks and cover its tracks to avoid detection.

At the bank, there were **no indications of trouble and no alerts that intruders had entered the system or taken control remotely**. It wasn't until February 5 that a problem was detected when the bank realized there were no SWIFT printouts that day. A full day went by and as manual printouts were made, the suspicious activity was revealed. It is believed the bank was not monitoring its systems against these kinds of threats. But as attacks and attackers evolve, security must evolve with them.

Timeline



The Bangladesh Bank heist illustrates the need for organizations to move from reactive to proactive security by focusing on three specific strategies:

1

Detect

Banks are under increasing pressure to detect what is known as well as unknown. Sophisticated new attacks demand a paradigm shift utilizing intelligent data science techniques to identify abnormalities internally to their environment and externally. They need to be constantly analyzing the attack landscape, actively looking for fraud and threats via financial as well as cyber indicators.

2

Prevent

Banks require a comprehensive security program which offers a defense in depth approach governing all spheres of cyber security: people, process and technology. To be effective, prevention must be multi-layered as attacks are today, to address and protect the specific business risks associated with the 'crown jewels' and their associated revenue streams.

3

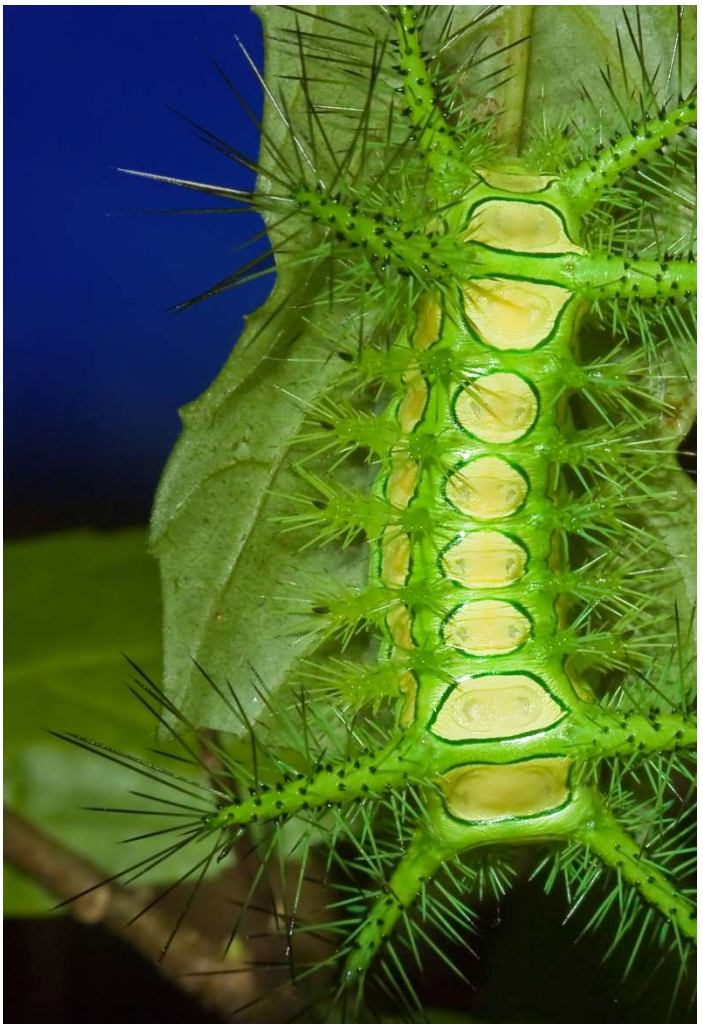
Respond

Banks must continue to evolve their cyber response capabilities to remain effective against these newer, focussed attacks. An experienced cyber response team will harness leading cyber response and forensic practices, such as database forensics, to better investigate and precisely scope advanced attacks like this one. It's not enough to stop the bleeding; banks must address root cause.

The threat landscape is ever changing.

Organizations can no longer rely on the same trusted techniques to adequately protect against new threats because the attackers know what works. There are state and non-state actors present who possess significant amounts of resources to create complex attacks which are neither easy to detect nor contain. The sophistication of attacks are increasing along with client and industry expectations, data protection and management expectations.

KPMG has assisted Banks in developing a Cyber Defensible Position. With improved threat hunting, security analytics and response capabilities, Banks can better detect, investigate and respond to incidents to limit impact.



Species such as the nettle caterpillar have adapted to ward off threats in the most challenging environments. Organizations also need to protect, detect and respond to ever-changing threats.

KPMG's Cyber Team can help your organization be cyber resilient in the face of challenging conditions.

Cyber Emergency?

Please contact our 24/7 Cyber response hotline

1-844-KPMG-911

1 (844) 576-4911

Contact us

Paul Hanley
Partner, National Cyber Security Leader
T: 416 777 8501
E: pwhanley@kpmg.ca

Kevvie Fowler
Partner, National Cyber Response Leader
T: 416 777 3742
E: kevviefowler@kpmg.ca