SWIFT banking system frauds shows that even trusted financial institutions are vulnerable to attack

May 20 2016, by Matthew Hollow, University Of York

Credit: AI-generated image (disclaimer)

A series of bank frauds using the SWIFT banking messaging service has revealed how even supposedly highly-secure financial institutions are vulnerable to attack through their computerised systems. An attack through SWIFT on Bangladesh Bank and a second on another un-named bank have been made public, but, as other reports of frauds linked to the SWIFT messaging system emerge in the US, Ecuador, Vietnam and Belgium, there is rising concern over the trustworthiness of financial transactions. Some have said that SWIFT is not fit for purpose.

The first attack on Bangladesh Bank was poised to steal around US$1 billion, but the hackers' ruse was discovered following their basic spelling error which led an automatic transaction to be checked by staff and stopped. Bank officials have since admitted that the attack was made possible after an official's computer had been compromised with malware.

Through the SWIFT messaging service, which transmits information about financial transactions worldwide, the hackers then sent a fraudulent message that purported to be a request from the central bank in Dhaka to transfer nearly US$1 billion from Bangladesh Bank's account at the New York Federal Reserve. The unidentified hackers were able to get away with US$81m before the scam was uncovered.

According to a report from security contractors BAE Systems, the hackers were able to use their access to the bank's SWIFT software to intercept messages about bank payments, manipulate displayed account balances and delete records of transfer requests. They were able to make fraudulent transactions and also conceal their actions until after the funds had been laundered. Had their poor spelling not let them down, it's likely that their ambitious sting would not have been detected until it was too late.

Financial crime in a digital age

SWIFT detected a second attack soon after without giving further details and has acknowledged that such incidents are not unknown:

SWIFT is aware of a number of recent cyber incidents in which malicious insiders or external attackers have managed to submit SWIFT messages from financial institutions' backoffices, PCs or workstations connected to their local interface to the SWIFT network.

This has caused much embarrassment and raised serious concerns about the security of the automatic electronic payment systems used worldwide today.

In 2015, a number of Russian banks were targeted by a gang using a malware called Metel that tampered with cash transaction records, meaning that almost unlimited amounts of cash could be taken out from cash machines undetected. Similarly, internet security firm Kaspersky discovered the Carbanak malware that granted hackers access to manipulate critical financial systems for their own advantage. The scale of the damage done by Carbanak is unknown, but is estimated to be well over US$300m worldwide.

These sorts of cyber-attacks pose a major threat because they target directly the systems and platforms banks use to communicate automatically with one another. SWIFT is used by banks to securely transmit information and transaction instructions to each other. Other similar systems are used for inter-bank transfers within countries – for example, BACS or CHAPS in the UK.

Naturally, every effort is made to ensure these networks are as secure as possible, with various checks on the transactions legitimacy made at both ends. Nevertheless, vulnerabilities do exist – particularly if a hacker is able to gain access to one of the many secure entry points in these networks.

No easy answers

Of course banks and financial institutions take cyber-security extremely seriously. One recent survey found that cyber-security is now the number one security concern for nearly half of financial institutions in the US.

But as banking becomes more automated and more interconnected, the growing number of points of entry to secure networks and their interconnectedness means that an attacker gaining access to one can access many others. International payment systems means that cyber-security failures in one part of the world can have consequences for systems in other, more secure parts of the world.

Ultimately, that so much of the financial system relies upon third-party services such as SWIFT means that even individual banks with exceptional security procedures can still be vulnerable to attack. Working out how to keep both the individual elements of the financial network, the banks and the communications systems and protocols that join them together secure will be a challenge that will keep the financial industry busy for a long time yet.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation

Citation: SWIFT banking system frauds shows that even trusted financial institutions are vulnerable to attack (2016, May 20) retrieved 17 July 2024 from https://techxplore.com/news/2016-05-swift-banking-frauds-financial-vulnerable.html