

\$US81m SWIFT hack highlights everyday security concerns - blueAPACHE

Canonical: <https://www.blueapache.com/blog/swift-hack-highlights-everyday-security-concerns>

Details:

Summary

This blueAPACHE post reports: In February 2016 during Chinese New Year, one of the most brazen and largest digital heists in history took place. A group of unidentified hackers used sophisticated malware to study bank workers and subsequently divert \$US81 million from a Bangladesh Central Bank account at the Federal Reserve Bank of New York to multiple accounts in Sri Lanka and the Philippines. It concerns emPOWER Security, emPOWER Core Network & Data Centre Interconnect, emPOWER Connectivity. Published in 2016. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2016
Services referenced	emPOWER Security, emPOWER Core Network & Data Centre Interconnect, emPOWER Connectivity
Cited figure	...Reserve Bank of New York to transfer funds. 30 transactions worth \$851 million were prevented by the banking system – but five requests were...

Article

The 2016 \$US81m heist (which could have been much worse!)

In February 2016 during Chinese New Year, one of the most brazen and largest digital heists in history took place. A group of unidentified hackers used sophisticated malware to study bank workers and subsequently divert \$US81 million from a Bangladesh Central Bank account at the Federal Reserve Bank of New York to multiple accounts in Sri Lanka and the Philippines. The instructions to steal the funds were issued via SWIFT – the Society for Worldwide Interbank Financial Telecommunication – a highly trusted and ubiquitous network used by thousands of financial institutions worldwide to facilitate transfers between banks. Computer security researchers have linked this theft to as many as 11 other attacks worldwide, all executed using the SWIFT banking network. The attacks involved malware written to issue unauthorised SWIFT messages and to conceal that the messages had been sent. In some cases, access was gained through targeted social engineering attacks that encouraged employees to inadvertently disclose their credentials and private access information. The hackers

managed to compromise Bangladesh Bank's system, observe how transfers are done, and gain access to the bank's credentials for payment transfers, which they used to send requests to the Federal Reserve Bank of New York to transfer funds. 30 transactions worth \$851 million were prevented by the banking system – but five requests were granted; totalling \$20 million to Sri Lanka (later recovered) and \$81 million lost to the Philippines. According to reports, the core messaging system of SWIFT was not breached; instead, the criminals attacked the banks' connections to the SWIFT network. Most banks have governance to identify fraudulent transactions, however the malware deletes evidence of the hackers' activities and subverts normal business processes to remain undetected.

Implications

Hackers are increasingly focusing on SWIFT and other private platforms. Aside from the greater transactional values (and fewer alarms for high value transactions), SWIFT's security is not equipped to deal with the progressively sophisticated attacks from modern day hackers. The 30 transactions that were prevented were typically halted through human intervention due to common spelling mistakes ("fundation" instead of "foundation" for example). According to BAE Systems, a defence and security company that analysed the attack, "the general tools, techniques and procedures used in the attack may allow the gang to strike again. All financial institutions who run SWIFT Alliance Access and similar systems should be seriously reviewing their security now to make sure they too are not exposed.

"The wider lesson learned here may be that criminals are conducting more and more sophisticated attacks against victim organisations, particularly in the area of network intrusions." Moving forward These attacks signal a warning not just for the SWIFT platform and financial institutions, but any organisation that deals with private platforms. Users of procurement, contract and payment gateways need to be cautious. Private platforms might feel safe, but as the value and awareness increases, targeted threats against specific organisations are becoming increasingly common and effective. The way your network is structured can potentially open up your entire data infrastructure to threats. Dividing the network into segments or placing data in separate disconnected networks may minimise the impact of a targeted attack. Intelligent network architectures can contain attacks and minimise damage automatically, moving organisations away from a reactive solution. The SWIFT hacking also serve as a grim reminder that cyber security is as much about people as it is about technology – with sophisticated hackers being able to recruit employees to hand over credentials and other key details. Cyber security awareness training is one of the most effective ways to prevent social engineering attacks. If employees know what to look out for, are vigilant, and question any suspicious information request, then they are less likely to become an unwitting accomplice to such attacks. If you have concerns about the threats of potential cyber-attacks on your organisation, or would like staff training on security awareness, contact the blueAPACHE account team .

Related

emPOWER Security

emPOWER Security (pillar)

emPOWER Core Network & Data Centre Interconnect

emPOWER Connectivity (pillar)

Frequently asked questions

How much money was ultimately stolen in the 2016 Bangladesh Bank SWIFT heist, according to the article?

The article says hackers stole \$81 million to accounts in the Philippines, plus a further \$20 million sent to Sri Lanka that was later recovered, out of 30 attempted transactions worth \$851 million that the

banking system prevented.

How did the article say the hackers gained access to issue the fraudulent SWIFT transfer requests?

The article says the hackers compromised Bangladesh Bank's system, in some cases through targeted social engineering that got employees to disclose credentials, then used the bank's own SWIFT payment transfer credentials to send fraudulent requests to the Federal Reserve Bank of New York.

What common error typically stopped the fraudulent transactions that were blocked, according to the article?

The article says the 30 blocked transactions were typically halted through human intervention due to common spelling mistakes, citing "fundation" instead of "foundation" as an example.

What did BAE Systems say about the risk of similar attacks recurring, according to the article?

BAE Systems, which analysed the attack, said the general tools, techniques and procedures used may allow the same group to strike again, and urged all financial institutions running SWIFT Alliance Access and similar systems to review their security.

Is the information in this post still current?

No. It reports a specific 2016 banking heist and its immediate aftermath; for blueAPACHE's current security services, see the emPOWER Security pillar page rather than this post.

Source

<https://www.blueapache.com/blog/swift-hack-highlights-everyday-security-concerns/>

Knowledge Base

What was the \$US81 million SWIFT hack described in your blog post?

In February 2016 during Chinese New Year, a group of unidentified hackers used sophisticated malware to study bank workers and divert \$US81 million from a Bangladesh Central Bank account at the Federal Reserve Bank of New York to multiple accounts in Sri Lanka and the Philippines.

How were the fraudulent instructions issued in the 2016 SWIFT heist?

The instructions to steal the funds were issued via SWIFT (the Society for Worldwide Interbank Financial Telecommunication), a highly trusted and ubiquitous network used by thousands of financial institutions worldwide to facilitate transfers between banks.

How much money did the hackers attempt to steal, and how much was actually lost or recovered?

The hackers attempted 30 transactions worth \$851 million, which were prevented by the banking system. Five requests were granted, totalling \$20 million sent to Sri Lanka (later recovered) and \$81 million lost to the Philippines.

How did the hackers gain access to Bangladesh Bank's systems and credentials?

The hackers compromised Bangladesh Bank's system, observed how transfers are done, and gained access to the bank's credentials for payment transfers, which they used to send requests to the Federal

Reserve Bank of New York to transfer funds. In some cases, access was gained through targeted social engineering attacks that encouraged employees to inadvertently disclose their credentials and private access information.

Was the core SWIFT messaging system itself breached in the attack?

According to reports, the core messaging system of SWIFT was not breached; instead, the criminals attacked the banks' connections to the SWIFT network. The malware deleted evidence of the hackers' activities and subverted normal business processes to remain undetected.

How were the 30 fraudulent transactions that were prevented actually stopped?

The 30 transactions that were prevented were typically halted through human intervention due to common spelling mistakes, such as 'fundation' instead of 'foundation.'

What did BAE Systems say about the implications of the SWIFT attack?

BAE Systems, a defence and security company that analysed the attack, said the general tools, techniques and procedures used in the attack may allow the gang to strike again, and that all financial institutions running SWIFT Alliance Access and similar systems should be seriously reviewing their security. BAE Systems also noted that the wider lesson may be that criminals are conducting more sophisticated attacks against victim organisations, particularly in network intrusions.

What network architecture recommendations does the blog post make in response to the SWIFT hack?

The blog post recommends dividing the network into segments or placing data in separate disconnected networks to minimise the impact of a targeted attack, noting that intelligent network architectures can contain attacks and minimise damage automatically, moving organisations away from a reactive solution.

What role does human behavior play in attacks like the SWIFT hack, according to the blog post?

The blog the SWIFT hacking serves as a grim reminder that cyber security is as much about people as it is about technology, since sophisticated hackers were able to recruit employees to hand over credentials and other key details. It recommends cyber security awareness training as one of the most effective ways to prevent social engineering attacks, so employees can recognize and question suspicious information requests.