nSEC/Resilience

IT Security IT Performance

Whitepaper

SWIFT Banking Hack

September 15th, 2016

Analysis of the 2016 "SWIFT Hack" – inadequate security testing or …?

With the experience nSEC/Resilience has in the banking industry, we were surprised to see a number of subsequent news reports asserting that the SWIFT network was hacked. As core banking systems are usually well secured, and response to security incidents is fast and thorough, it would seem logical that any successful penetration of the SWIFT network would be limited to one incident because the vulnerability would be addressed quickly. Have we overestimated the security of the global network for financial transactions? Are banks lazy and inadequate in their IT security?

The SWIFT network

The SWIFT network (Society for Worldwide Interbank Financial Telecommunication) enables banks and other financial institutions worldwide to send and receive information about financial transactions. SWIFT is also an organisation that provides software and services to financial institutions, related to the SWIFT Network. The BIC codes that sometimes are required for your own cross-border transactions are related to the standards of this SWIFT network.

It is already good to know that the SWIFT network does not actually transfer money; instead, it sends payment orders that have to be settled by the correspondent accounts that the participating banks have with each other.

Only banks can participate in the network. And a bank can only access the SWIFT network through the software application SWIFTNet Link. Other application, such as the bank's backoffice applications, all have to go through this SWIFTNet Link in order to communicate with the network. Adding the other top-grade security measures of SWIFT and the banks themselves, it is very difficult to actually hack one's way to the SWIFT network.

Attack details

So how did the attackers compromise the security?

In the case of the Bangladesh bank, where the hack was performed in February 2016, the main contractor in the forensic investigation of this breach (Mandiant) did shed some light on what actually happened. A representative was quoted to say that gaining access through the bank's outward facing systems is very unlikely. It is cheaper and more effective to exploit the human factor in security. Evidence was found that malware was already on the bank's systems in January. This would have given the attackers plenty of opportunity to collect information on typical transfers and username/password credentials of bank employees.

Although it is not clear how the malware was installed into the bank's systems, the properties of the malware and the way it was used did indicate that there was already a lot of information on the bank's organization structure and business processes. This would indicate that the malware infection was preceded by targeted social engineering attacks.

And although the details of it are out of scope of this discussion, extensive knowledge and preparation was required for the money laundering operation that enabled the transferred funds to actually become available and usable for the attackers.

Evaluation

In itself, SWIFT has many internal security controls that prevent abuse. For example, each message needs to have a specific code, which can be used to check whether the message has indeed been sent from a terminal that is part of the bank concerned. Realistically, attackers will need to get hold of valid codes and credentials to order transfer of funds through SWIFT.

This information indicates that, as is so often the case, the root cause of the successful attack lies in exploiting the human factor to get a beachhead in the target organization, instead of a direct technical attack from outside the bank.

Developing countries have different maturity levels for IT security than more developed countries. Although technical penetration testing will still help to further improve IT security for banks similar to the Bangladesh bank, the core technical security seems to already be adequate, and more attention will be required for measures against social engineering attacks and additional security controls around high-risk transactions. When banks have taken adequate measures in these areas, the threshold for attackers to execute similar attacks will be raised significantly.

About nSEC/Resilience

nSEC/Resilience was founded in 2013 by battle hardened test specialists, coming from both the functional testing discipline as the non-functional testing discipline.

nSEC/Resilience wants to provide complex test services such as security testing or performance testing in a more transparent and approachable manner, against high standards, with competitive prices.
Our services include penetration testing, training on IT security testing and security awareness, performance testing and test automation.

Would you like to know more about our services? Please contact us through our website: www.nsec-resilience.com.