When thieves strike

Executive briefing on the significance of SWIFT attacks and countermeasures

Executive briefing.
September 2016

pwc

In February 2016, one of the largest online heists in history was reported by Bangladesh Bank. An attempt had been made to siphon 951 million USD, with 81 million USD actually lost. The heist was reported to have occurred by targeting SWIFT alliance systems. Subsequently, a number of banks across the world have reportedly been targeted.

The biggest challenge with the SWIFT type of attacks is that most banks are taking point measures to respond to these attacks. However, point measures address only a specific attack vector while leaving multiple lacunae unaddressed. Many banks have undertaken reviews of controls of the SWIFT system, while some others are expecting certain anti-malware technology to protect them from such attacks. Although these are good measures, they are woefully inadequate. In order to develop suitable countermeasures, one first needs to understand the subtleties of this particular attack and what made it successful.

> ***"Point measures are inadequate to address SWIFT type of attacks in the long run."***

SWIFT is incidental!

Attacks such as the one we saw on SWIFT systems are complex and involve reconnaissance activity, development of custom code, propagation to target and, finally, the actions. In the SWIFT attack, we understand that the SWIFT alliance software was compromised using a sophisticated malware,[1]

> ***"Attackers have to cross multiple levels of security mechanisms for a successful attack."***

[1]BAE Systems report: http://baesystemsai.blogspot.in/2016/04/two-bytes-to-951m.html

However, looking at the broad spectrum of systems in a bank which are similarly vulnerable, this attack vector is not only incidental but also the last leg in possibly a series of compromises. What we need to realise about such attacks is that attackers had to cross multiple levels of security mechanisms to reach a system such as SWIFT. This means that every weak link—whether a compromised laptop, a third party, network, perimeter breach, failed access control, or lost mobile computing device—is an important stepping stone for the attacker.

We now know that quite detailed information was available with the attackers in the case of the Bangladesh Bank attack, including information regarding interfaces, arrangements with NY Fed Bank, and even printer make/model information. Barring insider involvement, this is possible only when previous breaches have led to data exfiltration. Sometimes data as innocuous as the printer make and model can make a difference to the success of the attack.[2]

SWIFT systems make better attack vectors than other systems, primarily due to their widespread use, well-known interface/message formats and universal knowledge of fund transfer processes. This knowledge makes the attack repeatable, and multiple banks can be targeted using the same modus operandi. Repeatability of an attack may be important when success rates are low. However, for a highly targeted attack, such constraints may not apply. This basically implies that every system within a bank which performs functions leading to the transfer of funds or change accounting entries is a target.

“Sometimes data as innocuous as the printer make and model can make a difference to the success of the attack.”

[2]As per the BAE report, the SWIFT malware used information on the specific printer model to prevent confirmation notifications from SWIFT being printed and hence avoid detection by the bank’s team.

Looking at comprehensive measures

We believe there is no reason why such attacks will subside over time. If at all, it is a wake-up call to most financial institutions on the types of threats which they need to be cognisant of. While we recommend certain immediate steps which all banks need to take, it is the long-term solutions which can make a difference to the cyber resilience of a bank. A few of the key aspects which banks need to address immediately include:

Immediate measures:

1. Perform malware analysis of persistent and volatile memory of important systems to detect any malware.
2. Monitor memory, processes and command execution on critical systems. Whitelist known processes and flag off any suspicious processes.
3. Review all controls pertinent to financial systems including, segregation, access and patch management.

Mid-term to long-term measures:

1. Strengthen the basic controls around network security, access management, data leakage, etc. It will be prudent for most institutions to take a very conservative approach to data sharing.
2. Create a capability to carry out real-time monitoring and analytics at the end point, especially focusing on process creation, with command line arguments and executable hash.
3. Start taking cognisance of the smaller breaches, malware infections, data exfiltration and other attacks which the bank faces on a regular basis. Develop the security operation centre's ability to correlate this vast amount of information and distil intelligence through pertinent use cases.
4. Enhance network monitoring controls, either through flow monitoring or full traffic inspection. It is worthwhile to use market available threat feeds to detect C2 connections. However, importantly, the bank will need to write its own use cases, or perform analysis to detect targeted malware C2 connections.
5 Develop capabilities to detect and analyse unknown malware. Develop threat intelligence in house. Develop capabilities to hunt malware.
6. Use baiting software such as PwC Flytrap to detect lateral movement of malware within the systems.

Conclusions

The nature of the adversary has changed: He is now an expert in business and technology. The use of sophisticated attacks and complex tools suggests a very well-funded and organised group with knowledge of the banking domain. The expertise exhibited in erasing the money trail suggests prior experience in large-scale money laundering.

The adversary is patient, focused and willing to develop complex attacks. It is not possible to defeat such an adversary through strategic moves and tactical measures. *The primary tool of a security professional should be a threat model and security strategy which describes the attack vectors and the preventive, detective and response mechanisms.*

Finally, it is essential that banks address security both from a technical and business point of view. The security of business processes, their confidentiality, third-party risks, access, etc., need to be balanced against a need for market agility and convenience.

Security is as strong as the weakest link.

For more information, contact:

Sivarama Krishnan
Leader, Cyber Security
+91 9650788787
sivarama.krishnan@in.pwc.com

Sangram Gayal
Director
+91 9819197716
sangram.gayal@in.pwc.com

ME/September2016-7440