TLP WHITE

Advisory: Bangladesh Bank hack and SWIFT

CUK-23-04-16-CD 26.04.2016

Introduction

CERT-UK is aware of open source reporting an incident in February 2016 in which hackers stole $81m from a Bangladeshi bank. Recent reports indicate the attackers were able to gain access to Bangladesh Bank's SWIFT payment orders system, the system used for securely transmitting information and instructions among financial institutions. They were able to steal the $81m by leveraging this system and cover their tracks in the process.

Background

BAE Systems has identified a malware that was bespoke for attacking Bangladesh Bank's infrastructure which also had the capability to manipulate the legitimate internal SWIFT system. BAE concluded their report[1] with the following:

"This attacker put significant effort into deleting evidence of their activities, subverting normal business processes to remain undetected and hampering the response from the victim."

BAE also concluded that they were still unclear how the malware was implanted. It has however been widely reported that the bank in question was using 'cheap' internet routers and had no firewalls. While the true method of attack is not yet known, the suggested attack vector indicates a poor security culture, which likely explains why the attackers were able to gain access to this bank's network.

In response, SWIFT reported that this malware only targets affected institutions' local environments and has no impact on its wider network or core messaging services. In order to install malware on a victim's network, malicious actors must identify and exploit weaknesses in a victim's own local environment. In this regard, CERT-UK does not assess that SWIFT itself was compromised or that it was the root cause of the network breach. However, once this malware is in the network, given its capability to leverage the legitimate SWIFT systems, the organisation has released a mandatory update which provides additional integrity verification and alerting capabilities.

An institution's internal systems are only as secure as the network itself. If an attacker breaks into a network, as was the case here, then it is probable a malicious actor could manipulate legitimate internal processes, such as those run by SWIFT software, for monetary gain.

Mitigations

CERT-UK recommends that all financial institutions who run SWIFT Alliance Access and similar systems should:

1. In the context of this attack; review and potentially adjust the architecture within which SWIFT Alliance Access sits to ensure that countermeasures are appropriately deployed.

2. Ensure that network countermeasures such as IDS and A/V products which protect the networks are explicitly configured to detect evidence of this malware.

3. Review monitoring processes to ensure that evidence of this malicious activity will be escalated quickly.

[1] http://baesystemsai.blogspot.co.uk/2016/04/two-bytes-to-951m.html?m=1