Attack Brief: Bangladesh Bank SWIFT Attack

Who was attacked?

Bangladesh Bank is the central bank of Bangladesh. With 5,807 employees, the bank is one of over 11,000 financial institutions, from 212 countries, that use the SWIFT messaging system to send and receive financial-transaction information. Every day, the SWIFT system is used to transmit billions of dollars globally.

What was the attack narrative?

In February 2016, $81M was stolen from the Bangladesh Bank via its account at the Federal Reserve Bank in New York. $951M of fraudulent SWIFT transactions would have been processed, and were only prevented by happenstance: a spelling error in the recipient line of a fraudulent message (the word "Fundation") was seen by a bank employee.

How did the attack operate?

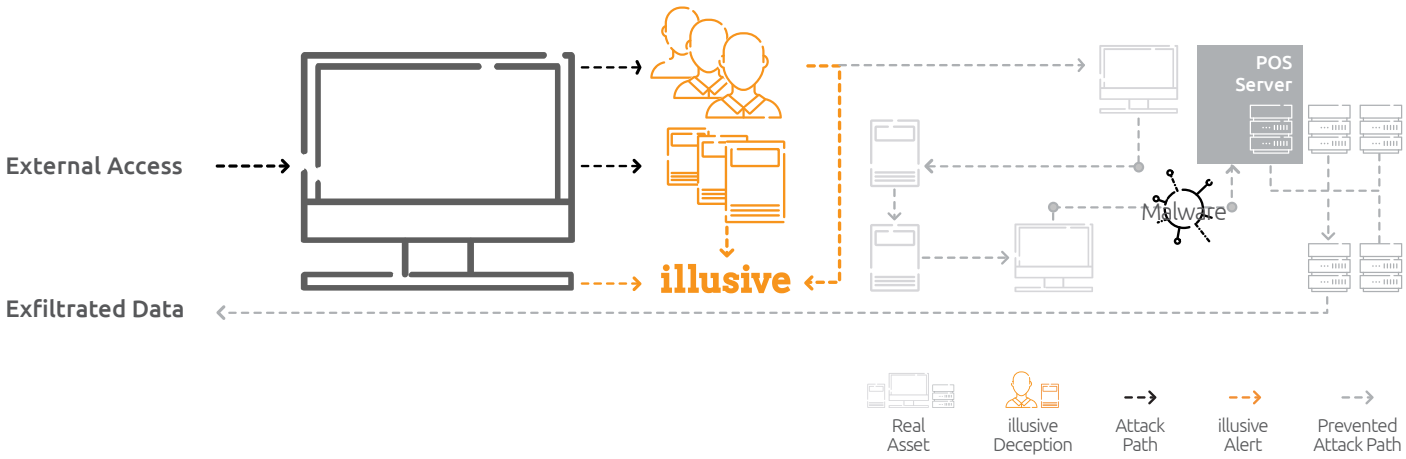
According to a New York Times report, the attack was traced to penetration of one of the SWIFT system components: the SWIFT Alliance Access software, which handles financial messages before they are sent to the SWIFT interface.

To locate the SWIFT system on the bank's network, attackers first executed an APT attack that lasted one year and involved various malware programs. Having compromised a single host, the attackers diligently moved laterally from host to host, exploring the network.

When the SWIFT system was finally located, attackers monitored how SWIFT messages were processed and sent this information to a C&C platform. The platform hard-coded the bank's SWIFT resources into a malware program that successfully sent fraudulent SWIFT messages. To avoid detection, attackers learned that bank protocol involved printing SWIFT messages for review. Therefore, the malware program was designed to hide fraudulent messages from digital logs and delete them from printed lists of transfers.

How would illusive have detected the attack before the payload launch?

Prevention Through Detection



The illusive Deceptions Everywhere® solution would have detected the advanced attack in real time and immediately collected forensics from compromised hosts, which would have allowed Incident Response teams to prevent attackers from reaching sensitive data.

The SWIFT Guard™ would have detected the SWIFT attack as it occurred, ensuring that the bank's finances and brand remained safe.

- illusive coats hosts with deceptive credentials, network locations, and secure connections, ensuring that attackers reveal themselves as they attempt lateral movements.
- illusive deploys dedicated deceptions that constitute fake SWIFT systems, diverting and revealing attacks that attempt to access real SWIFT systems.