2018 - A Cyber Attack on Marriott Hotels

- What happened?
  - Leaked originated from StarWood reservation system. System was compromised unusual database query SQL injection attack. The database query was made by a user with administrator privileges, but analysis quickly revealed that the person to whom that account was assigned was not the one who made the query; someone else had managed to take control of account.

- What is the effect?
  - Hackers were able to copy more than 5.25 million unencrypted passport numbers and 383 million booking records. Additionally, the hackers stole 8.6 million encrypted credit card numbers and 20.3 million encrypted passport numbers, which were protected as long as the encryption holds. Once the damage was done, it was one of the largest data breaches in history.

- How did it happen?
  - Investigators began scouring the system for clues, and discovered a Remote Access Trojan (RAT) along with MimiKatz, a tool for sniffing out username/password combos in system memory. Together, these two tools could have given the attackers control of the administrator account. It's not clear how the RAT was placed onto the Starwood server, but such Trojans are often downloaded from phishing emails, and it's reasonable to guess that might've been the case here.

- How did they solve the problem?
  - Put in place defense in depth to counter against too few layers of defense
  - Put in more access controls
  - VPN

- How can we prevent this from happening again?
  - Hold off the firing of Starwood's IT staff, until system is in full transition and in controlled by new IT department.
  - Set up Intrusion Protection/Detection System, using stronger Encryption Algorithm and Monitoring system.
  - Set up Penetration Testing Exercise to discover vulnerabilities in system software.

Done by [SCTP Cohort-4] :
Joseph Ong
Muhammad Rudyn
Richie Chia