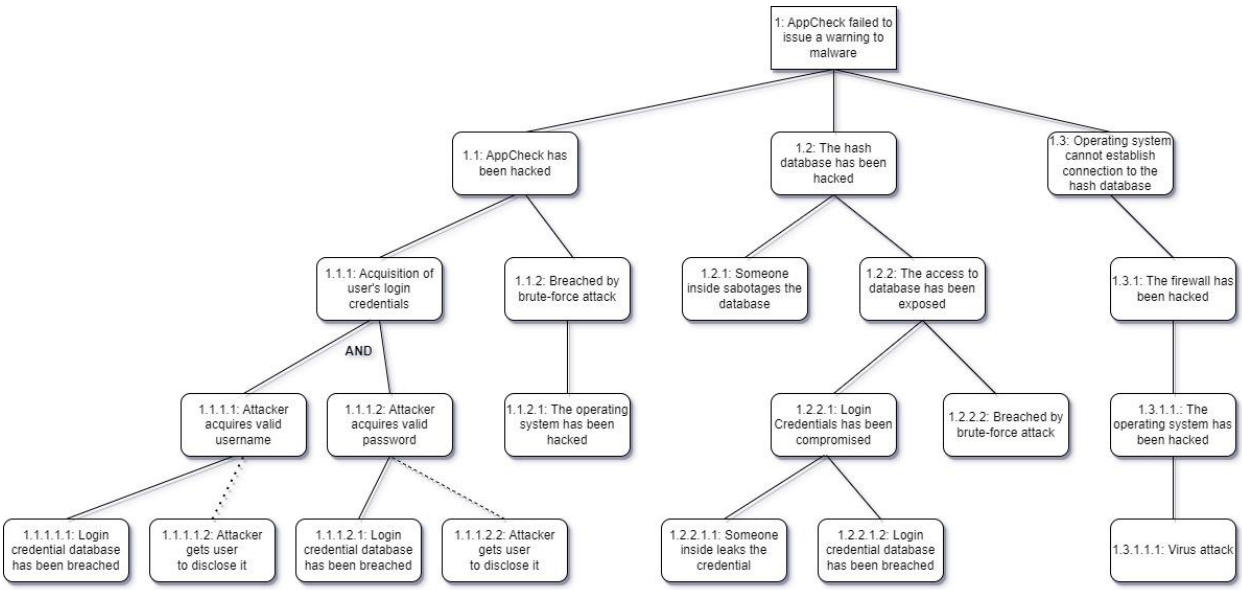
Report

Leshan Wang 201388927

Description

According to the given scenario, the attack tree is constructed which majorly considers three valid attack categories, with eight distinct attack paths, as shown below. A straight deduction from failure of warning infers problem is either on the user-end, or on the database-end. On the user-end, it could be AppCheck's self-malfunction, or the application is interfered by operating system's problem. On the database-end, the chances are errors occurred and lead to malware detection failure on user-end. It is most likely that these errors are all results of intentional attacks.



The Most Possible Attack Path

Among the eight attack paths, the path of virus attack which leads to hacking of operating system and firewall is most likely to succeed. In this scenario, a cyber virus intrusion has not been detected or stopped. The virus is designed to undermine AppCheck's ability of malware detection by adding rules to

firewall to block the application's access to the hash database. By doing this, AppCheck could no longer get up-to-date hash information about newly published software, thus unable to identify malware which pretends to be an existing popular software (it might notify user the software is unknown).

For the other scenarios: a crack on AppCheck itself requires either breach of local database that stores user login credentials, or brute force cracking the application. The first approach requires sophisticated hacking techniques, and the other one is too noticeable; compromission of hash database is even more difficult, considering the cyber security company is very likely armed with advanced and secured protective solutions, nor an inside betrayal is likely to occur. Therefore, a stealth attack on user-end firewall is more valid.

Mitigation

To prevent this attack from happening, it would be reasonable if a routine firewall check function is added to AppCheck.

By simply scanning implemented rules and newly added rules, user could identify any sign of malicious firewall activities in time. After excluding this possibility, attackers would have to turn their focus on cracking AppCheck itself, which is clearly much harder.