# Threat Agent Identification Example

### Identifying Threat Agents

The process of identifying a threat agent:

1. Take the list of all sensitive data (or information to protect) listed in Section 2.
2. Make a list of the different ways to access this data.
3. Create a list of the different agents (i.e., persons, technologies, and processes) that could be used to access the data. These are your threat agents.

One way to understand how to identify threat agents is to use an example of a financial application,specifically a banking application. Following the identification process as previously stated:

1. Sensitive data present in the application has been listed as: beneficiary details stored in some form in the phone application memory and user credentials used for authentication transmitted to the server.

2. List the various ways of accessing information:
    A. Beneficiary details:
        i. A device user aiming to browse through the memory card/phone memory
        ii. An adversary using a jailbroken phone; starts reading the content through putty/WinSCP via SSH
        iii. An adversary while sniffing the Wi-Fi traffic sniffs the content travelling through the network
        iv. Another malicious application while reading the phone memory contents, stumbles upon this data as the device is jailbroken
        v. Another application which is sending data through SMS sends this data.

        vi. A Web application executing a script on the browser tries to steal the phone memory and send it to its server.

3. From the above points, we list the medium used:
    A. Any user who has the device (stolen device/friend/etc.)
    B. Any malicious application (installed/web-based script)
    C. An adversary sniffing the Wi-Fi.

From the above example, management should have a clear picture on how to identify threat agents. Below is a list of possible threat agents identified while analyzing commonly used applications.