BlackRock Android Malware

Why in News

Recently, a security firm has alerted about a **new malware called BlackRock** which targets social, communication, and dating apps.

Key Points

- BlackRock is a **banking Trojan** and said to be an enhanced version of existing **Xerxes malware** which itself is a variant of the **LokiBot Android trojan.**
    - A **trojan** is any type of malicious program disguised as a legitimate one. Often, they are designed to steal sensitive information (login credentials, account numbers, financial information, credit card information, and the like) from users.
    - Banking trojans are a specific kind of trojan malware. Once installed onto a client machine, banking trojans use a variety of techniques to create botnets, steal credentials, inject malicious code into browsers, or steal money.
- **Functioning:** It collects user information by abusing the Accessibility Service of Android and overlaying a fake screen on top of a genuine app. It uses Android DPC (Device Policy Controller) to provide access to other permissions.
- **Concerns:**
    - It surfaces as a **google update.**
    - The malware is said to have the design to overlay attacks, send, spam, and steal SMS messages as well as lock the victim in the launcher activity. It can also **act as a keylogger** (i.e. track the keys struck on a keyboard), which essentially could help a hacker to acquire financial information.
    - Despite being a banking Trojan, BlackRock is said to **target non-financial apps.**
        It targets a total of 337 apps, which is significantly higher than any of the already known malicious code.
    - It **makes antivirus applications useless.**

Source: IE