



## Eventbot : a Mobile banking trojan



- Abuses Android's in-built accessibility features to steal user data from financial applications, read user SMS messages and intercepts SMS messages allowing malware to bypass two-factor authentication.
- It uses several icons to masquerade as a legitimate application such as Microsoft Word, Adobe flash etc. and using third party application downloading sites to infiltrate into victim device
- Once installed on victim's Android device, it prompts user to give access to device's accessibility services
- It can also read LockScreen and in-app PIN that can give attacker more privileged access over victim device.

### Safety Measures:

- Do not download and install applications from untrusted sources. Install apps downloaded from reputed application market
- Verify app permissions and grant only those permissions which have relevant context for the app's purpose.
- In settings, do not enable installation of apps from "untrusted sources"
- Avoid using unsecured, unknown Wi-Fi networks.

**A V Rama Rao**  
**General Manager**