Android.Banker.A9480 Trojan

It has been reported that a malicious application targeting various banking and payment apps [including Indian banks] has been circulating. The malicious application is masquerading as Flash Player which is being offered via third party app stores. It asks user repeatedly for granting Administrator's rights unless user allows. The application steals banking credentials, intercept SMSs, displaying an overlay screen (to capture details) on top of legitimate apps, steal sensitive data to attacker controlled servers, among others.

Once successfully installed **after being granted administrative privileges**, it listens for command from the Command and Control (C&C) server and keeps track of the installed applications. If the targeted payment applications found, the app shows a fake notification on behalf of the targeted banking app with the app's icon. If the user clicks on the notification leads to a phishing page of the targeted bank to steal the user's confidential.

Upon receiving specific commands from the C&C server, the app can do activities in the background like intercept SMS's to thwart OTP based authentication, can collect all the contacts and SMS on the device and siphon off to the C&C server, can send specific SMS on the mobile contacts, can send IP/GPS location etc.

Best Practices

Do's

- Install / update the Anti-Virus software regularly with the latest patches.
- Always update apps manually on regular basis.
- Install apps from trusted source like google play store/Apple store etc and Disable installation of apps from unknown sources in your Mobile Security Settings
- Enable auto lock feature in phone
- Use SIM lock feature
- Password protect your memory card
- Enable mobile tracking and report lost phone immediately
- Do factory reset in case phone is given to another user or before discarding.
- Make sure to use strong passwords/pattern lock/biometric lock in all apps wherever feasible.
- Password/patterns should be changed periodically.
- Check the type of file attached in the mail before opening it. Avoid opening file with unknown extension.
- Always installed licensed version of OS.
- Uninstall all unwanted apps.
- Keep your Bluetooth, wifi, mobile internet, hot spot, NFC off in case not needed.
- Hide your device from getting it searched across network.

- Scan your mobile for untrusted application on regular basis and uninstall the same immediately.
- Delete any unwanted file from mobile after uninstalling any app.
- Keep your data encrypted if supported by device.
- Scan your device before and after connecting as USB device.

Don’ts:

- Do not open unknown email attachments on mobile.
- Do not open any untrusted link/website
- Do not allow permission to update apps automatically.
- Never download apps from un-trusted sources, even if they are appealing.
- Never store any personal information like passwords, PIN, credit/debit card detail etc. in any app.
- Never provide permission to any app which is not necessary for the app and review permission on regular basis.
- Do not give Administrator’s Rights to any app even if it asks repeatedly
- Do not use unsupported Operating system and apps.
- Do not installed freeware apps on your Mobile.
- Do not use removable media devices on systems.
- Do not use untrusted WiFi/Bluetooth connection.
- Do not use multiple apps for financial transactions.
- Do not root your mobile phone.
- DO not use admin user on mobile if multiple users are supported in mobile
- Do not allow notification access to all apps