

Subject: Advisory - Prevention Against Cyber Espionage (Advisory No. 17)

1. **Introduction.** WhatsApp has recently launched video calling feature. Because of popularity of WhatsApp hackers are taking advantage and sending false emails and messages to install malicious app in the garb of enabling WhatsApp video feature.

2. **Malicious Link**

a. **C&C Servers**

Ser	URL	IP	Country	Registrant Country
(1)	http://whatapp.videocalls.co	193.124.189.79	USA	Mumbai, India
(2)	http://Whatsapp.com.oyc.videocallactive.co	185.87.50.216	USA	Mumbai, India

3. **Analysis**

- a. Reported links are developed by Indians therefore it is evident that Indian hostile agencies are attempting to hack mobiles of Pakistani users.
- b. Malware can take control of mobile and extract data, picture to C&C server abroad.

4. **Recommendations**

- a. If the user has ever clicked a link to enable WhatsApp video call feature, it is strongly recommended that phone be reset to factory default settings to remove malware.
- b. Please do not click or share such links in future.
- c. Keep your phone up to date including OS and all apps from official source.
- d. Only install WhatsApp from Google play store.
- e. If you receive any request or text from unknown users on WhatsApp, please do not proceed further without proper authentication.