PAKISTAN REVENUE AUTOMATION (PVT.) LTD.

329

Dated: Thursday, February 22, 2018

ADVISORY NOTICE

Malicious URL in WhatsApp Group

A malicious url 'blocked.win' is getting popular in WhatsApp groups and social media. The website claims that after installation of the (fake) application, it can show you the contacts who blocked you on WhatsApp. The website asks the user to share its link with 14 users or 7 WhatsApp groups for downloading of malicious Android executables, which will ultimately hack user's phone.

Password Stealing Apps on Google Playstore

Recently, the security researchers have discovered around 85 Android applications on Playstore that are designed to steal credentials from users of Telegram (instant messaging service) and VK (a Russian based social networking service).

Malicious North Korean Cyber Activity

Reliable reports reveal release of joint technical alerts on malicious North Korean cyber activity, referred as Hidden Cobra. North Korea is actively targeting the media, acrospacc, financial and critical infrastructure sectors. Tools and capabilities used by Hidden Cobra actors include DDOS botnets, key loggers, RATs and wiper malware.

Some of the precautionary measures and recommendations to prevent this security risk are listed below:

Recommendations:

1. FBR IT Security Policy must be strictly followed. Copy can be obtained from FBR IT Wing.
2. Do not download attachments from emails and messengers unless sure about the source.
3. Use of official email is recommended.
4. Maintain regular offline backups or centralized offline back of your critical data.
5. Do not click on the link to restrict the advisory from getting the location.

/328/

6. Regular update the Android OS and its application.
7. Update all third party applications and hardware with latest patches.
8. Enable Google Play Protect security feature on the device. This feature will remove (uninstall) malicious apps from user's Android smartphone to prevent further harm.
9. Contact your local PRAL technical support team for any assistance.
10. In case of infection/compromise in your computer system by your phone or other media, please disconnect the computer from internet and immediately contact PRAL Support Team.

This advisory notification is being issued on the pretext of letter no. 6(3)Coord/2004-Misc., dated 30th January 2018, of the Cabinet Secretariat, Cabinet Division, National Telecom & Information Technology Security Board (NTISB-II).

Further information about online security threats and support, please contact PRAL Networks & Infrastructure Department at:

Landline	(051) 9259358
IP Phone	1234
Email	stpsupportteam@pral.com.pk datacenter@pral.com.pk

DEPARTMENT OF
NETWORKS & INFRASTRUCTURE
PRAL

Distribution to:

- FBR House, Islamabad
- All FBR IR & Custom Offices
- PRAL Head Office, Islamabad