Pakistan Revenue Automation (Pvt) Ltd.

Plot #: 156, Software Technology Park
Service Road (North), Sector: I-9/3,
Islamabad
Ph. 051-9259435, Fax: 051-9259356

No. PRAL/CEO/ 462

Date: 02-04-2018

335

Syeda Adeela Bokhari
Chief (IT)
Federal Board of Revenue
Islamabad

Subject: **ADVISORY – PREVENTION AGAINST CYBER ESPIONAGE (ADVISORY NO. 110, 111 & 112)**

Please refer to your emails, dated 26th March 2018 regarding the subject.

As per recommendations from Cabinet Secretariat, Cabinet Division, National Telecom & Information Technology Security Board (NTISB-II) via their advisories, all employees of FBR should be informed regarding the serious risks pose by:

a) A new Android spyware 'Skygofree' that provides hackers full control of infected devices remotely.
b) Utilization of hacked websites for the generation of crypto-currencies to earn money.
c) A malicious email titled 'Promotion List' containing malware that affects computer systems.

Enclosed please find Advisory Notice (Annex-I), which may be circulated within FBR with the purpose of creating precaution and data safeguard awareness among FBR officials.

Additionally, as we are receiving frequent advisories from government agencies, therefore it is suggested that these advisory notices may be posted online at FBR's website as well, in order to keep FBR personnel aware of the latest cyber security threats.

Important
For necessary
compliance

Mohammad Imran Amjad
Chief Executive Officer

Encl: As above.

Send to
webmaster,
&
Sec Pr via chief FATIE as directed
suggested by CEO-PRAL

3.4.2018

on file DFA
SPtdt
3.4

Secretary 4

PAKISTAN REVENUE AUTOMATION (PVT.) LTD.

e334

Dated: Monday, April 02, 2018

ADVISORY NOTICE

A new Android spyware 'Skygofree'

A new Android spyware 'Skygofree' has been found that provides hackers full control of infected devices remotely. Skygofree is capable of taking pictures, capturing video, and seizing call records, text messages, geolocation data, calendar events, and business-related information stored in device memory.

Utilization of hacked websites

Recently, malware writers are utilizing hacked websites for the generation of crypto-currencies to earn money. Hackers, embed malicious scripts into the compromised website so that they can make use of visiting user's CPU resources to mine crypto currency.

A malicious email titled 'Promotion List'

A malicious email titled as 'Promotion List' is being sent to officers and staff of Government departments. The email contains a malicious .doc file. Downloading and opening the file executes malware in the background that results in hacking of the computer.

Some of the precautionary measures and recommendations to prevent these security risks 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. Use of third party Antivirus is strictly prohibited. Only PRAL approved licensed Antivirus software must be installed on desktops.
6. Keep Windows firewall enabled on your desktops systems.

7. Do not click on unknown hyperlinks to restrict the advisory from getting the location.
8. Regular update mobile and desktop Operating Systems.
9. Update all third party applications, software and hardware with latest patches.
10. Enable Google Play Protect security feature on the Android device. This feature will remove (uninstall) malicious apps from user's Android smartphone to prevent further harm.
11. Contact your local PRAL technical support team for any assistance.
12. 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 letters no. 1-5/2003(NTISB-II) (Advisory No. 110,111 & 112), dated 16th March 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