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/ 1104

Date: 02-08-2018

Mr. Abbas Ahmed Mir
Chief (IT-BDT)
Federal Board of Revenue
Islamabad

Subject: **MULTIPLE ADVISORIES BY NTISB (ADVISORY NO. 138 TO 144).**

Please refer to multiple advisories via pretext no. 1-5/2003(NTISB-II), dated 20th July 2018.

1305-SS(BDT-IT) 3-8-18

As per recommendation from Cabinet Secretariat, Cabinet Division, National Telecom & Information Technology Security Board (NTISB-II) via their advisories (Advisory no. 138 to 144), all employees of FBR should be informed regarding the serious risks pose by online threats and hazards.

Enclosed please find Advisory Notice, 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.

for 02/08/18

03/08/18

Mohammad Imran Amjad
Chief Executive Officer

SS(BDT-IT)

Encl: As above.

P(process as per previous practice

07/8.

Asstt. C(IT)

PAKISTAN REVENUE AUTOMATION (PVT.) LTD.

Dated: Thursday, August 02, 2018

ADVISORY NOTICE

(Advisory no. 138) Prevention against Vega Stealer

Security researchers have discovered a new malware named 'Vega Stealer' developed to steal saved login and credit card credentials from Chrome and Firefox browsers. Apart from credential stealing capability, the malware also steals sensitive documents from the targeted device.

(Advisory no. 139) Prevention against Hacking of Social Media Accounts

It has been observed that there is a rise in hacking of social media accounts since last one year due to lack of awareness on usage of internet and mobile.

(Advisory no. 140) Prevention against Cyber Espionage

United States Computer Emergency Readiness Team (US CERT) has published two alerts regarding attack by North Korean government referred to as 'Hidden Cobra' targeted towards businesses sensitive and proprietary information. This targeted malicious attack has affected large number of countries.

(Advisory no. 141) Prevention against Cryptoiacking Malware

A new malware attack capable of Cryptojacking has been discovered is targeting mac devices. Cryptojacking is a form of cyber-attack in which a hacker hijacks a target's processing power in order to mine cryptocurrency.

(Advisory no. 142) Prevention against IoT Botnet Malware 'VPN Filter'

Security researchers have discovered highly sophisticated Internet of Things (IoT) botnet using malware 'VPN Filter' to hack IoT devices. Malware has affected more than half a million routers and storage devices in many countries.

(Advisory no. 143) Prevention against Cyber Espionage

A critical vulnerability has been found in 'Cortana' an artificial intelligence-based smart assistant that Microsoft has built into all version of Windows 10, allowing cyber criminals to unlock your system password and access the system.

(Advisory no. 144) Prevention against threats posed by Wireless Router

Wireless Routers poses serious security threats as it may allow anyone in close proximity to access your complete network and monitor traffic by hacking the router.

Recommendations:

1. FBR IT Security Policy must be strictly followed. Copy can be obtained from FBR IT Wing.
2. Maintain regular offline backups or centralized offline backup of your critical data.
3. Use of third party Antivirus is strictly prohibited. Only PRAL approved licensed Antivirus software must be installed on desktops.
4. Keep Windows firewall enabled on your desktops systems.
5. Regular update Operating System, Antivirus software, Internet browsers and MS Office, and disable macros.
6. All sensitive information be handled with care and dissemination to all concerned be done through secure means.
7. Use of official email is highly recommended.
8. Avoid clicking unknown links and downloading attachments sent by anonymous users.
9. Be aware of pop-ups in internet browsers or desktop screen and never enter confidential information in a pop-up screen.
10. Check your online accounts and bank statements regularly to ensure that no unauthorized transactions have been made.
11. Avoid using free WiFi available at public places.
12. Change the passwords of your respective accounts regularly.
13. Always memorize the passwords, never write it.
14. Turn off GPS function on your smart phone while at work.
15. Always download mobile applications from App stores and avoid third party sources.
16. Always scan suspicious file using PRAL approved Antivirus software.
17. Contact your local PRAL technical support team for any assistance.
18. 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.

The advisory notification is being issued on the pretext of letter no. 1-5/2003(NTISB-II), dated 20th July 2018.

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