Sunday, May 01, 2022

ADVISORY NOTICE

Prevention against Fake FBR Emails

National Telecom and Information Technology Security Board (NTISB) has warned the Federal Board of Revenue (FBR) that government job advertisement-related emails are being sent to unrestricted users by hackers with the purpose to acquire confidential information and a potential cyberattack on government institutions.

A phishing email with the subject "Govt Jobs/ Recruitment" which contains a malicious Word document as an attachment is being spread by Hackers. On downloading the attachment: a malware runs in the background. It is a spearphishing attack conducted by Confucius APT Group to gather information at a large scale through a Biodata form.

On downloading the malicious email attachment, an individual's computer/device is compromised and the hacker gains access to all the stored data/files. End users are urged to withhold from downloading attachments or clicking links sent via such enticing emails in order to protect their personal information.

Recommendations:

- 1. FBR approved IT Security Policy must be strictly followed. A copy can be obtained from FBR IT Wing.
- 2. Do not open attachments in suspicious or strange emails especially Word, Excel, PowerPoint, or PDF attachments.
- 3. Verify the sender by checking their email address. Call the sender if you have high suspicion.
- 4. Check the link, before you click, make sure the links start with HTTPS:// and not HTTP://.



PAKISTAN REVENUE AUTOMATION (PVT.) LTD.

- 5. Be careful when providing personal information, never provide your credentials to third parties.
- 6. Do not rush or panic reacts, scammers use this in order to pressure you into clicking links or opening attachments.
- 7. If you gave sensitive information, do not panic. Reset your credentials on sites you have used them. Change your passwords and contact your bank, etc. immediately.
- 8. Preferably delete the suspicious email without opening it and manually block the sender.
- 9. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of any intrusion. It is highly recommended that the computer system must be registered with LAN's Active Directory server. Please contact your local technical support for further details.
- 10. Use of official email is highly recommended.
- 11. Use of third-party Antivirus is strictly prohibited. Only approved licensed Antivirus software must be installed on computer systems.
- 12. Always avoid using a suspicious USB flash stick. In case you still want to use the USB flash stick, then always scan the USB using approved Antivirus software.
- 13. Regular update Operating System, Antivirus software, Internet browsers, and MS Office, and disable macros.
- 14. Keep Windows firewall enabled on your desktop computer systems.
- 15. All sensitive information be handled with care and dissemination to all concerned be done through secure means.
- 16. Change the passwords of your respective accounts regularly.
- 17. Always memorize the passwords, never write them.
- 18. Maintain regular offline backups or centralized offline backups of your critical data.
- 19. Be aware of pop-ups in internet browsers or desktop screens and never enter confidential information on a pop-up screen.
- 20. Contact your local PRAL technical support team for any assistance.



PAKISTAN REVENUE AUTOMATION (PVT.) LTD.

21. In case of infection/compromise in your computer system, please disconnect the computer from the internet and immediately contact PRAL Technical Support Team.

For further information about online security threats and support, please contact PRAL Networks & Infrastructure Wing at:

Information & Support During Office Hours		Information & Extended Support 24x7	
Landline	(051) 9259358	Landline	(051) 9212374 (051) 8431155
IP Phones	1234 1400	IP Phones	1492 1155
	Email: datac	enter@pral.com.p	k

Distribution to:

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

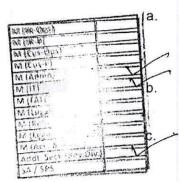
GOVERNMENT OF PAKISTAN CABINET SECRETRIAT CABINET DIVISION (NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad 25th April 2022

Subject: -Advisory - Fresh List of Malicious Appls (Advisory No. 14)

- Sequel to already identified 70x malicious apps, 8x new malicious apps 1. (PaighamChat, Skymate, Boss, ChitChat Box, Triover, Hideme, LionVPN & Zepp) are being used by Hostile Intelligence Agencies (HIAs) for espionage/ information gathering. Newly identified applications are chat-cum-hacking apps developed by Indian Military Intelligence to trap armed forces and civil persons to extract classified information through technical/ coercive (blackmailing) measures.
- 2. Individuals who have accidently installed any of malicious apps mentioned in Appendix-I must immediately perform following actions: -



Note down contact details (WhatsApp number/ Facebook ID etc) of suspected individual who shared the link for downloading the application for reporting the same to CSO of own organization/ department.

Immediately switch off infected mobile phone (remove battery if possible), remove SIM and disconnect from internet.

Share subject information/ incident with all persons/ saved contacts for their security.

3. Recommendations. Above in wiew, following best practices recommended: -

> Always check application permissions before installation of application and install applications from Google Play Store only.

> Under command should regularly be sensitized about malicious actors' tactics, techniques and procedures, moreover, all personnel (officers/ staff) be sensitized to refrain from engaging in activities that may lead to exploitation.

> Install and update reputed antivirus solution on Android devices like AVAST or Kaspersky. After installation, scan the suspected device with antivirus solutions to detect and clean infections.

> Before downloading/installing apps on Android devices, review the app details, number of downloads, user reviews/ comments and "ADDITIONAL INFORMATION" section.

2005 civing 28/1/22

Revelved in Chairman's Sectt on 2-6-APR-2622

- e. In mobile settings, do not enable installation of apps from "Untrusted Sources".
- f. Install Android updates and patches as and when available from Android device vendors.
- g. Do not download or open attachment in emails received from untrusted sources or unexpectedly received from trusted users and forward them to emails mentioned in para 4.
- Avoid using insecure and unknown Wi-Fi network as hostile elements use Wi-Fi access points at public places for distributing malicious applications.
- Use two-factor authentication on all Internet Banking Apps, WhatsApp, social Media and Gmail Accounts.
- All officers/ staff must be guided to adhere recommended cyber security measures at personal smart appliances.
- 4. For any query or reporting malware, please forward the same on following email address:
 - a. eagle1978@mail.com
 - b. falcon098@writeme.com
 - c. asntisb2@cabinet.gov.pk
- 5. Disseminate the same message in your organizations, all attached/affiliated departments and ensure necessary protective measures.

Major (Muhammad Usman Tariq) sistant Secretary-II (NTISR)

Assistant Secretary-II (NTISB) Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments.

Copy to: -

- 1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
- 2. Secretary to the President, Aiwan-e-Sadar, Islamabad
- 3. Cabinet Secretary, Cabinet Division, Islamabad
- 4. Additional Secretary-III, Cabinet Division, Islamabad
- 5. Director General (Tech), Dte Gen, ISI Islamabad
- 6. Director (IT), Cabinet Division, Islamabad

LIST OF IDENTIFIED MALICIOUS APPLICATIONS

Ser	Name of Appls	
1.	Fruit Chat	
· 2.	Just You	
3.	CuCu / CUCKOO-	
4.	Rapid Chat	
5.	Islamic Chat	
6.	Vmate	7
7.	Lite Chat	
8.	Chat On	
9.	Chat It	
	Philions Chat	
	Phub	
	Zoiper	
	Seta/ SA News	the state of the s
14	Safe Chat	
	Tweety	
	Rocket Chat	
	Pornhub	
	FMWhatsAPP	
19.		
20.		
21.		The state of the s
	Graphic Version	
	VIBES	
24.		
	Buzz Version 3	
	Filos	
27.	Quran.Apk	
	Secure[t/ Spitfire	
	Buzz	
	Guftagu	
31.	Xpress	
	U & Me	
	TeleChatty	
34.	Babble/ Babble Ver	3
	Chirrups	
36.	Converse	
	Free VPN V3	
38.	Face Call	
39.		
40.	Twin Me	
41.	Hex Chat	
42.	FaceChat	
43.	Omegle	
	Zaning V4	
	Pvt Chat	
	Privantechat1	
	Secure Chat	
	Safe Dialer	
	Crypto Chat	
70.	Crypto Chat	

50.	SecureIt	
51.	Wire	
52.	Google Security Framework	
	Cable-1	And the state of t
54.	Privee Chat	
55.	FireChat	
56.	Stumped	
57.	Zong Chat (Beta)	
58.	Buddy Chat	
59.	Media Services	The second second
60.	CrazyChat	
61.	ZangiV2	
62.	Zapme	
63.	CuCU Chat	
64.	Chat 24/7	
65.	ZongBoost	V. 1
66.	Audio & Video Recorder	
67.	Kakao Talk	
68.	Love Bae	100 100 100
	Easy Chat	
70.	ISPRNews	
	PaighamChat	
72.	Skymate	A
73.	Boss	H T
74.	ChitChat Box	(18)
75.	Triover	
76.	Hideme	
77.	LionVPN	
78.	Zepp	