

Subject: - Cyber Security Advisory – Fake/Malicious Website Spoofed as Legitimate Government Website (MoIT&T/FIA) (Advisory No. 01)

Introduction. A new spoofed website impersonating as legitimate government website (MoIT&T/FIA) used for hacking purposes (spreading via SM channels) by hacker groups has been identified. Details of spoofed websites are as follows:

Ser	Website	Purpose	C&C/IP	Linkage
a.	https://moitt-govv-pk.fia-gov.net	Hacking bait via spoofing	77.83.196.59 (HZ Hosting Ltd, Poland, Europe)	SideWinder APT (India)
b.	https://moitt-gov-pk.fia-gov.net/364896null/file.rtf			

2. Mitigation. Above in view, please avoid opening/testing above mentioned websites. Also, IT administrator are requested to blacklist said website/C&C servers (where applicable).

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

23 FEB 2024

C(IT)