

Subject: - Cyber Security Advisory - Cyber Attacks Against Pakistan by Sidewinder APT Group (Advisory No. 54)

Context. Advanced Persistent Threat (APT) groups are generally stealthy threat actor that attacks cyber infrastructure of other states to gain unauthorized access/ingress while remaining undetected for an extended period of time. Usually, APTs are state sponsored group e.g. Sidewinder is an Indian APT group that has often targeted Pakistan's military and civil setups. Profile, modus operandi and preventive measures of APT groups are given in the subsequent paras.

Fdx 1/4

28 DEC 2022
C(A&F)

S(Koopd) 29/11/22
S(16/4/22)

MAI/HR

2. Sidewinder APT Group

- a. Profile. Sidewinder (also known as Rattlesnake and T-APT-04) is an Indian APT group present in cyberspace since 2012. The APT group came into limelight in 2018 when various cyber security researchers identified its modus operandi and its nefarious operations.
- b. Modus Operandi. Sidewinder primarily targets the Asian Region. It mainly uses spear phishing emails and masquerading techniques (crafted websites, emails and mobile apps) to execute cyberattacks on regional countries including Pakistan.

Forward to
Chief (IT).
Section 4/11/23

Previous Activities - Pakistan

- (1) Incident Analysis and Investigation reveals footprints of Sidewinder in Critical Govt departments.
- (2) The APT Group relied on spear phishing email attacks including fake covid-19 emails and Govt department's fake emails with embedded malware to conduct cyber espionage operations. In this regard, numerous advisories were issued to all concerned highlighting the attack pattern of Sidewinder.

26/29/22
FBR eDOX By No
Revised in Chairman's Sectt
on 27 DEC 2022

Current Activities - Pakistan. Recently, Sidewinder has evolved its attack capabilities after likely having access to legitimate mailing systems. Masquerading techniques include; illegally using identity of Pakistani Govt Legitimate/trusted users and websites such as NADRA & Pakistan Air Force to infiltrate other systems and gain PII of Pakistani users. The masquerading techniques are based on compromising Govt email systems and forwarding fake emails/letters for data extraction/infiltration and compromise.

- (g) Implement MFA in mailing systems administrator controls and other critical systems.
- (h) Always maintain back up of critical data periodically.
- (i) Regularly change passwords at administrative level.
- (j) Regularly patch and update all OS, applications and other technical equipment.

c. Users

- (1) Always re-verify trusted user who has sent email/attachment via secondary means (call, SMS, verbal) before downloading.
- (2) Report any suspicious activity to the Administrator immediately.
- (3) Never keep critical data on online systems and store it in standalone systems.

4. For any query or reporting malware/cyber incident, please forward the same on the following email addresses: -

- a. Falcon1947@proton.me
- b. asntisb2@cabinet.gov.pk

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