Subject: - **Cyber Security Advisory - Patchwork An Indian APT Group (Advisory No. 49)**

Context. Advanced Persistent Threat (APT) groups are anonymous threat actors attacking Cyber/IT infrastructure of other states to gain unauthorized access/ingress while remaining undetected for an extended period of time. Usually, these groups (Sidewinder, Bitter, DoNot etc.) are Indian state sponsored that often target Pakistan's Military and civil IT setups. Recently, **PatchWork (an Indian APT group)** has actively targeted Chinese and Pakistan State Institutions for data exfiltration. In this regard, profile, modus operandi, indicators of compromise (loCs) and preventive measures are as under:

2. **PatchWork - Indian APT Group**

a. **Profile**. PatchWork (also known as Mahabusa and White Elephant) is an Indian APT group present in Cyberspace since 2015. The APT group came into limelight in 2017 when various Cyber security researchers identified its modus operandi and nefarious operations.

b. **Modus Operandi**. PatchWork primarily targets Asian Region. It mainly uses spear phishing emails, whaling, social engineering and masquerading techniques (crafted malicious emails, fake rating websites appearing to be legitimate to gain users trust and SM links to download malicious mobile apps) to execute Cyber-attacks on regional countries including Pakistan and China.

c. **Malware Type/Exploit (loCs)**

(1) Android RAT
(2) Bad News RAT
(3) File Stealer Malware Delphi

d. **C&C Servers**. Following details/associated URLs have been revealed during investigation:

Ser	Domain
(1)	Filepiece.com
(2)	Techwatch.com
(3)	Bingoplant.live

e. **Malicious Attachment/Documents**

Ser	MDS
(1)	2c3b9984be2d8609f83d10171a4f1059
(2)	f9ad3d4c90528e654de20159859ca15b
(3)	5a2265017b8083d540f274f16038c6df
(4)	893060bff7da03f5555ecc9931d0c700

f. The C&C servers URLs may be processed for blocking at local firewalls.

3. **Preventive Measures**. An APT group may frequently change its techniques, tactics and procedures. However, phishing email remains initial entry point for malicious activities. Therefore, few preventive measures (but not limited to) are:

a. **Anti-phishing Guidelines**

(1) Never share personal details and credentials with unauthorized/ suspicious users, websites, applications etc.

(2) Never install unknown and suspicious applications.

(3) Never click on unknown links and attachments.

(4) Always type URLs in browser rather than clicking on links.

(5) Always open websites with https and avoid visiting http websites.

(6) Never use personal accounts on official systems.

(7) Do not follow web links in emails to avoid Social Engineering and Phishing Attacks. Train users to recognize and report phishing attempts.

(8) Use multi-factor authentication (MFA)/two-factor authentications where possible.

(9) Regularly review applications permission, system running processes and storage utilization.

(10) Use reputed and licensed business email gateways, anti-phishing and anti-spam solutions.

(11) Always scan every document before opening/downloading via built-in anti-virus on mailing servers.

(12) Application whitelisting be ensured by allowing only specified applications to run and block all other applications.

(13) Organizations should have a timely vulnerability detection and patch management program in place.

(14) End-point protection systems to be kept updated and Windows Defender should always be active to ensure that malware execution is hindered.

(15) Timely update all applications and operating systems (PC and mobiles etc)

(16) Use separate and complex passwords for each system, mobile, SM accounts, financial and mailing accounts etc.

(17) Disable execution of PowerShell/Command line for normal users through Access control and Active Directory.

(18) Auto execution of VBScripts should be disabled and .docx/.docm files should never be clicked/opened.

(19) Use well reputed and updated anti-virus/antimalware for computer/ mobile

(20) Disable macros on documents (MS Excel, MS PowerPoint, MS Word etc.

b. **Anti-Masquerading Guidelines (Administrators)**

(1) Monitor networks including file hashes, file locations, logins and unsuccessful login attempts.

(2) Use reputed firewalls, IPS/IDS and SIEM solutions.

(3) Use separate servers/routing for offline LAN and online networks.

(4) Restrict incoming traffic and user's permissions to maximum extent by implementing system hardening at OS, BIOS and application level.

(5) Allow internet access to specific users on need basis and restrict data usage/applications rights.

(6) Verify software and documents before downloading via digital code-signing technique.

(7) Implement MFA in mailing system’s administrator controls and other critical systems.

(8) Regularly change passwords at administrator level.

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 administrator immediately.

(3) Never keep critical data on online systems and store it in standalone systems.

(4) Always create a back-up of critical data and store in external drives or standalone systems.

(5) Keep strong passwords on BIOS, OS level, drives (via bit locker).

d. **Blocking of Malicious Domains/URLs**. Block all malicious domains, URLs and hashes of documents at firewall/network including APT PatchWork. Have access to latest hacking threat intelligence forums and feeds to remain update with attacker's innovations regarding evasion techniques.