Subject: **Prevention Against Indian APT Group Sidewinder (Advisory No. 22)**

1. **Introduction.** Since Jan 2019, a suspected **APT group from India** is utilizing modern payloads and spoofed emails to target defense / government departments of Pakistan, to gain persistent access and sensitive information. These emails portray an interesting political topic and contain a malicious link for further information that redirects the user to download a zip file which contains a malicious lnk (shortcut) file. Downloading and clicking the shortcut file, opens a legitimate document in foreground and executes malicious code in background that gives unauthorized access to the hacker.

2. **Summary of Malicious Email**

   a. **Email Subject.** Key Discussion Points During Summit Between India and China

   b. **Spoofed Email address.** DGPR <dgpr.paknavy.gov.pk@email.com>

   c. **Download Package.** Key Points.zip

   d. **Antivirus Detection Rate.** 02/55 (3.63%)

   e. **File Size.** 3KB

   f. **File extension.** Zip (archival file format)

   g. **Download Address.** http://www.paknavy.gov.pk.ap1-port.net/images/E7B62E1D/1182/2258/fc8fe2b4/692cd02.

   h. **Classification.** Sidewinder APT Malware

   i. **Reference.** https://brica.de/alerts/alert/public/1249067/sidewinder-apt-organizations-disclosure-of-attacks-on-south-asia/

3. **C&C Servers**

Ser	URS address	IP address	IP Location
a.	https://www.paknavy.gov.pk.ap1-port.net	185.243.115.65	Germany
b.	https://asp-bin.net	185.99.133.140	New zealand

4. **Indicators of Compromise**

   a. C:\ProgramData\audacity2.2\credwiz.exe.

   b. C:\ProgramData\audacity2.2\Duser.Dll.

   c. C:\ProgramData\CommonsFiles\write.exe.

   d. C:\Users\Blah\AppData\Local\Temp\Key_Points.doc.

   e. C:\ProgramData\CommonsFiles\PROPSYS.dll.

5. **Capabilities of Malware**

   a. Malware has capability to bypass antivirus and windows whitelisting.

   b. The malware is specially designed for targeted attacks and can steal backup files, stored usernames and passwords.

   c. It can automatically execute itself on windows restart and every instance of this malware has extremely low detection rate.

6. **Recommendations**

a. Block execution of **mshta.exe, wmic.exe, cipher.exe and wscript.exe** on every system running in enterprise environment as **this attack relies on free execution of mshta.exe.**

b. **Block execution of power shell encoded and malformed commands or block execution of windows power shell altogether.**

c. Implement strict **Software Restriction Policies/ Application Whitelisting** to **block unsigned executable** running from **% AppData%,\StartMenu\ Programs\Startup* and % TEMP% paths.**

d. **Enable 2 factor authentication on all your email accounts** (Gmail, Yahoo, Hotmail etc), **social media accounts** (Facebook, Whatsapp etc) **especially internet banking** to prevent any sort of unauthorized access and finaical loss from this attack.

e. **Regularly maintain and update antivirus solution** from reputed vendor.

7. Forwarded for perusal and dissemination of information to all concerned and under command, please.