Subject: - **Cyber Security Advisory – Prevention against Espionage via Typosquatting Attacks (Advisory No.49)**

Context. It has been observed that cyber actors are using malicious websites with **names similar to the names of legitimate government websites**. The fake websites' names comprises of **common misspellings** or **short-names** of government websites (called **typosquatting attack**) to deceive users to unwittingly download files hosted on malicious link. Downloading and executing such files will compromise endpoint leading to attacker gaining access to system.

2. **Analysis**

a. **Attack Vector**. Social Engineering via emails to download malicious files from legitimate looking NTC website.

b. **Download Link**. http://finance.gov.pk.ntc-gov.com

c. **File Name**. File (circular_29092022.iso) is related to "Circulars" or "Notifications" dispatched to government setups regarding deduction of 2x day salary for flood relief victims.

d. **Package Details**. Malicious ".iso" files further contains following 3x additional files:-

(1) circular_29092022.pdf (Circular for flood relief)

(2) circular_29092022.pdf.lnk (link [LNK] file to execute malicious payload **NisSrv.exe**).

(3) NisSrv.exe (Malicious payload).

e. **Botnet/C&C Communication**. Following IPs are used for bot/C&C communication: -

(1) 51.210.32.103 (France).

(2) 54.145.6.146 (USA).

f. **Malware Capabilities**

3.

(1) Ability to download additional payloads.

(2) Bypass User Access Control with legitimate windows utilities like cmd.exe, powershell.exe etc.

(3) Upload files and stored usernames/passwords to C&C server.

4. **Recommendations**

a. Regularly update antiviruses such as Kaspersky, Avira, Avast etc and scan system regularly.

b. Update all software including Windows OS, Microsoft Office and all other on regular basis.

c. Uninstall all not in use applications and software from system and personal phones.

d. Do not download attachments from emails unless you are sure about the source.

e. Open Source tools and scripts such as **dnstwist (https://github.com/eleceef/dnstwist)** must be regularly used to **enumerate possible malicious domains** aiming at a typosquatting attack. Such domains (once found) must be **blocked** through **PTA**.

f. **Awareness campaigns** be carried out by all organizations/departments to **educate their officials** about such attacks.

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