GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT,CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003 (NTISB-II) **Islamabad 16 July, 2018**

Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 133)**

1. **Introduction.** **DNS Hijacking malware** is reported to target **i0S, Android** and **windows** users. Attackers can change the DNS settings of the wireless routers and redirect traffic to malicious websites for malware installation.

2. **Technical analysis**

a. **Roaming Mantis** is a malware that can hijack internet **routers** and distribute malwares to connected devices using DNS Hijacking.

b. Whenever users attempt to access website via compromised router, they are redirected to rogue websites, which serves:-

(1) **Sites with crypto currency mining script** to desktop users, **fake apps infected with banking malware** to Android users.

(2) Phishing sites to iOS users.

c. To evade detection, fake websites generate new packages in real time with unique malicious apk files for download, and also set filename as eight random numbers.

d. Malware steal sensitive information from Android and iOS devices, and injects a browser-based **crypto currency** mining script on each landing page if visited using desktop browsers.

3. **Affected Product Versions.** The malware effects **i0S, Android** and **windows users.**

4. **Mitigation Measures.** Following best practices are suggested in this regard:-

a. Ensure installation of latest version of the firmware and strong password access to network routers.

b. Disable router's remote administration feature and **hardcode "1.1.1.1." DNS server IP** address into the operating system network settings.

c. **It** is advised to make sure the sites you are visiting has **HTTPS enabled.**

d. **It** is advised to check if **Wi-Fi router** is already compromised, review DNS settings and check the DNS server address. If it does not çnatch the one issued by service provider, change it back to the right one. Also change all account passw9rds immediately.

e. Install apps/ software only from official stores. It's wise to **disable installation of apps from third-party sources.**

f. Always pay attention to misspelled app names, small numbers of downloads, or dubious requests for permissions-any of these things should raise flags.

g. Install a reliable security solution, for example, Kaspersky Internet Security, Avast Anti-Virus, Semantic etc. This will protect your device form malicious ap and files, suspicious websites, and dangerous links.

h. Be careful while using social media groups/pages and don't click or download any file or image.

i. Keep all the softwares, browsers and operating system up-to date.

5. Forwarded for perusal and dissemination of information to all concerned, please.

Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments