Subject: **Advisory - Prevention Against Windows Banking Trojan "Emotet" (Advisory No 46) Aug 18**

1. **Introduction.** A **malware** named **"Emotet"** has been spreading through **emails, social media** and targeting **windows** based users. This malware is **highly sophisticated, undetectable banking trojan** capable of stealing **sensitive** information causing **disruption** to regular operations.

2. **Technical Analysis**

a. **Emotet** is an advanced, modular banking Trojan that primarily **functions** as **downloader** or **dropper** of other **banking Trojans.**

b. Malware use several **methods** for maintaining **persistence,** including auto-start registry keys and services.

c. It uses modular **Dynamic Link Libraries (DLLs)** to continuously evolve and **update** its **capabilities.**

d. Malware can also evade **signature based detection** mechanism due to its **polymorphic** design.

e. Malware is spreading via **posts** on **Facebook groups, malspam** (emails containing **malicious** attachments or links) and **whatsApp messages** encouraging users to visit hackers-controlled fake websites.

f. **Emotet artifacts** are typically found in **arbitrary paths** located at **AppData\Local** and **AppDataRoaming** directories.

3. **Mitigation Measures.** Following **mitigation** measures are suggested in this regard:-

a. Use **Group Policy Object** to set a **windows Firewall** rule for restricting **inbound SMB** communication between **client systems.**

b. Use **antivirus programs,** with **automatic updates** of **signatures** and software, on **clients** and **servers.**

c. **Vendors** release **security patches** times to time, apply **appropriate patches** and **software updates immediately.**

d. Implement **filters** at the **email gateway** to filter out emails with known **indicators;** such as known **malicious subject lines** and **block suspicious IP** addresses at the **firewall.**

e. **Formulate** a **policy** regarding **suspicious emails** so that all suspicious **emails** should be **reported** to the **security** or **IT Department.**

f. Provide **employees** basic **cyber security** awareness **training.**

4. **Recommendations**

a. **Install** and **update** well reputed antivirus such as **Kaspersky,** Bitdefender, Nod32 and **Avast** etc.

b. Regularly update all software's including **Windows OS, Microsoft** Office and all other software's.

c. Strictly follow all **mitigation measures** mentioned at **para 3.**