SECRET

Subject: **Advisory - Prevention Against IoT Botnet Malware "VPNFilter" (Advisory No 40)**

1. **Background.** Security researchers have discovered highly **sophisticated IoT botnet** using malware **"VPN Filter"** to hack **IoT devices.** Malware has affected more than **half a million routers** and **storage device** in many of countries.

2. **Technical Analysis.**

   a. The malware has capabilities to **gather intelligence,** interfere with internet **communications,** as well as conduct **destructive cyber-attack** operations.

   b. **VPNFilter** is a **multi-stage** malware that can steal **website credentials** and **monitor industrial controls** or **SCADA** systems, such as those used in**electric grids,** other **infrastructure** and factories.

   c. The malware communicates over **Tor anonymizing** network with its **command and control(C&C)** server.

3. **Affected Products.** The following **routers** and internet-connected **storage devices** are known to be affected by this threat:-

   a. Linksys.

   b. MikroTik.

   c. NETGEAR.

   d. TP-Link.

4. **Mitigation Measures.**

   a. In case user of devices mentioned at **para 3,** reset router to **factory default** to **remove** the potentially **destructive malware** and **update the firmware** of your device as soon as possible.

   b. It is advised to remain **vigilant** about the security of **smart IoT** devices.

   c. It is recommended to change **default credentials** for **IoT devices.**

   d. If router is **vulnerable** and cannot be **updated** it is advised to **discard** the device.

   e. Always install routers behind a **firewall.**

   f. **Internet service providers** that provide **routers** to their users may **reset** and **update firmware** of the routers for their customers.

5. **Recommendations.**

   a. Strictly follow all **Mitigation measures** mentioned at **para 4.**

   b. Keep all **unnecessary services** and **ports blocked** in network connected devices.

   c. Permanently **disable** remote administration feature.

   d. **MAC/ IP bind** access to devices for **administration** purposes.

e. Regularly visit firm **website** for **security updates** released by the vendor. Enable all **built-in security** features provided by the **manufacturer.**