Subject: **Advisory – Prevention against Malicious ASUS Update (Advisory No.13)**

1. **Introduction.** A massive supply chain attack from infected ASUS Update Server has compromised more than 6 million computers worldwide. These malicious updates have been delivered via legitimate ASUS server and the malicious updates have **legitimate digital certificate** from **"ASUSTeK Computer Inc", making it nearly impossible for antimalware solutions to detect this malware centric update.**

2. **Summary of Cyber Attack**

   a. **Name of Malware**. Shadow Hammer.

   b. **Type of attack**. Watenng Hole attack (In this attack, hackers compromise widely used software or website).

   c. **Affected Product**. Asus Computers.

   d. **Type of Malware**. Windows Backdoor.

   e. **Capabilities of Malware**. After hacking the ASUS update server, hackers distributed malware to end users via ASUS update utility:-

      i. The malware distributed by ASUS update server had **legitimate digital certificate which made them appear authentic.**

      ii. By using said malware, the **hackers gained unrestricted access to infected endpoints.**

3. **Recommendations**. In this regard, following measures are recommended:-

   a. **Kaspersky has released an endpoint detection tool** at this link **https://kas.pr/shadowhammer, to check the presence of this malware (Shadow Hammer), to check the presence of this malware (Shadow Hammer).** ASUS users are strongly advised to **download and run this automated tool for detection of this infection.** If your computer is affected then backup your data and reinstall windows.

   b. **Install and update well reputed antivirus solution** like Kaspersky, AVAST, Avira etc and make sure that real time protection feature is enabled.

   c. Make sure that both host-based firewall and network-based firewalls are operational.

   d. **Don't use Internet Explorer or Microsoft Edge as they might be susceptible for browser hijacking**. It is recommended to utilize Google Chrome or Mozilla Firefox for internet surfing.

e. **Never install 3rd party malicious plugins in web browser excep like Adblock or Adblock plus.**