Subject: - **Cyber Security Advisory – Malware Targeting Unsigned vSphere Installation Bundles (Advisory No. 44)**

Context. A malware targeting computer systems through **vSphere** has been identified. In case of successful exploitation, an attacker can gain administrative privileges and use unsigned **vSphere Installation Bundles (VIBs)** to inject backdoors on a compromised **ESXi host**.

2. **vSphere Product**. VMware is **VMware's cloud computing virtualization platform**. It includes a **vCenter Configuration Manager, vCenter Application Discovery Manager** and **vMotion** to move more than one virtual machine from one host server to another.

3. **Capabilities of Malware**

   a. Maintains **persistent administrative access** to hypervisor.

   b. Sends commands to hypervisor to route to guest VM for execution.

   c. Transfers files between **ESXi hypervisor** and guest machines.

   d. **Tampers logging services** on hypervisor.

   e. Execute arbitrary commands from one guest VM to another guest VM running on the same hypervisor.

4. **Recommendations**. Administrators of vSphere are advised to enable Secureboot feature in ESXi. In case of any issue, product vendor may be approached for enabling Secureboot. Further, to avoid malware propagation, hardening of vSphere be ensured through following steps (**but not limited to**):-

   a. **Network Isolation**. At time of configuring network settings on ESXi hosts, only enable VMkernel network adapters on isolated management network.

   b. **Identity and Access Management**

      (1) **Decoupling ESXi and vCenter Servers** from Active directory.

      (2) Use **vCenter Single Sign-On**. Enforce multi-factor authentication (MFA) for all management access to vCenter Server instances and store all administrative credentials in a Privileged access Management (**PAM**) system.

   c. **Services Management**

      (1) Restrict services and management of ESXi hosts, implement lockdown mode, this step will ensure that ESXi hosts can only be accessed through a vCenter Server.

      (2) Configure the built-in ESXi host firewall to restrict management access only from specific IP addresses.

   d. **Log Management**. Ensure all ESXi host and vCenter Server logs are being forwarded to the organization's SIEM solution.