Subject: **Prevention Against Ramsy Malware (Advisory No.11)**

1. **Context.** Access to air gapped system AFs / strats setups has always been a focus of advisories to exploit. A cyber-espionage campaign is spreading Ramsay malware through USBs, portable media, shared drivers, websites, unwanted software etc. This malware is currently being used in targeted campaigns only, as very few sightings of this malware have been seen / reported. Its major target is data rich servers especially air-gapped networks.

2. **Summary of Cyber Threat**

   a. **Type.** Data Collection and Exfiltration especially through Air Gapped Networks.

   b. **Known Attack Vectors**

      (1) Malicious Word Documents with Vulnerability (CVE-2017-0199).
      (2) Emails and SMS.
      (3) USBs and other removable / portable medial / software installer.

   c. **Capabilities / Features.**

      (1) System info collection (IP Address, Mac address, Hostname etc.).
      (2) Has ability of privilege escalation via UACMe instances (Can change permissions from Standard user to admin.
      (3) It can collect screenshots and document files (doc,.pdf,.ppt, .text).
      (4) Scans for network shares / removable drives (main propagation vectors).
      (5) Ramsy can hook itself into various auto-execute locations and can automatically execute itself on system restart (DLL Injection, Registry etc.).

   d. **Detailed Analysis and Report**. https://www.welivesecurity.com/ 2020/05/13/ramsay- cyberespionage-toolkit-airgapped-networks/

3. **Recommendations / Mitigations.**

   a. Install latest, wellreputed and licensed antimalware solution on all systems especially Windows operating within organization.

   b. Install ad blockers on Windows browsers to combat exploit kits and malicious advertising.

   c. All operating systems and applications should be kept updated on a regular basis.

d. Legacy systems operating within organization should be replaced via new operating hardware with latest security measures and updated patches.

e. Always update / download software from official resources.

f. Restrict execution of PowerShell / WSCRIPT in an enterprise environment.

g. Ensure installation and use of the latest version of PowerShell within organization with centralized monitoring of commands, if PowerShell is not required by the end user then block its execution on endpoint.

h. Establish a Sender Policy Framework (SPF) for your email domain to prevent spam by detecting email spoofing through which most of the ransomware samples successfully reaches the corporate email boxes.

i. Implement strict application whitelisting to block binaries running from %APPDATA% and %TEMP% paths. Malware sampledrops and executes generally from these locations.

j. Don't open email attachments received from unknown sources. and in case of any hacking activity, information be sent on email ID: **asntisb2@cabinet.gov.pk**.

k. Block the attachments of file types, exe|pif|tmp|ur|vb|vbe|scr|reg|cer| pst |cmd|com|bat|dll|dat|hlp|hta|js|wsf.