Subject: **Advisory - Ransomware Attacks (Advisory No. 36)**

1 Introduction. Recently, malicious cyber actors deployed **Dark Side ransomware** against a US pipeline company ICT network that heavily crippled country's gasoline supply. Consequently, a **state of emergency in 18x USA states** was declared. Cyber threat actors also **stole 100 GB of data** and leaked it online even after an amount of USD 54 was paid as ransom. In light of this devastating attack, it is urged that network / system administrators of critical organizations must follow recommendations mentioned in **para 3** to prevent against the ransomware attacks.

2. Technical Details

a. **Attack Vectors.** Cyber threat actors used attack vectors such as Phishing Emails, Remote Desktop Protocol **(RDP)** and Known Vulnerability exploitation.

b. **Attack Tools, Tactics & Procedures (TTPs).** Following TTPs were used:-

(1) **PowerShell:** for **reconnaissance** and **persistence**

(2) **Metasploit Framework:** for reconnaissance

(3) **Mimikatz:** for reconnaissance

(4) **BloodHound:** for reconnaissance

(5) **Cobalt Strike:** for installation

(6) **7-Zip:** a utility used for **archiving files** for exfiltration

(7) **Rclone** and **Mega client: tools** used for exfiltrating files to cloud storage

(8) **PuTTy:** an application used for network file transfer.

c. **Mode of Operation**

(1) After gaining access; DarkSide actors deployed DarkSide ransomware to **encrypt** and **steal sensitive data.**

(2) The actors then threaten to publicly release 100GB of data if the ransom is not Paid.

(3) Even after ransom of 5 million dollars was paid, the attackers did not provide the decryption key and leaked the data.

3. **Recommendations**

a. **System / Network Administrators.** In order to prevent from ransomware attack, **application whitelisting** is the **key** and must be applied at all endpoints along with following additional measures:-

(1) Windows commands / utilities not required by end-users such as like mshta.exe, bitsadmin.exe, finger.exe, certutil.exe,cipher.exe and syskey.exe **should be blacklisted for endpoint execution.**

(2) **Block execution of scripts** having extension .vbs, .vbe, .hta, tjs, .wsh, .wsf, com, .pif, .psi extensions.

(3) **Blacklist / block outbound network connections** from winword.exe, notepad.exe, explorer.exe, powershell.exe, bitsadmin.exe, Imshta.exe, excel.exe and eqnedt32.exe.

(4) Block execution of powershell and command prompt, if explicitly not required by the endpoint.

(5) Centralized **monitoring of endpoint windows logs** must be performed to detect anomalous user behavior.

(6) Cyber threat actors may continue to innovate new techniques, launch new attacks and create new strains of crypto -malware. Therefore, it is essential to have **access to reputable threat intelligence feeds**.

(7) Always implement multi-factor authentication for remote network access via VPN service.

(8) Regularly **update antimalware solutions running on endpoints** in enterprise environment as well as standalone systems.

(9) Educate endusers regarding cyber security best practices and antimalware measures.

(10) Ensure that data backups are regularly taken and duly verified.

b **<u>End-users</u>**

(1) **Regularly update well reputed antiviruses** such as Kaspersky, Avira, Avast etc. and scan system regularly.

(2) **Do not download attachments from emails or websites unless you are sure about the source.**

(3) Avoid downloading software from untrusted websites or torrents.

e. Use Chrome / Firefox browsers for surfing internet instead of Internet Explorer.

f. Make sure that web browser is up-to-date and no plugins other than adblock or adblock plus are enabled.

* * * * *