Subject: - **Cyber Security Advisory - Dead Glyph Backdoor (Advisory No. 63)**

Advanced Persistent Threat (APT) groups are targeting global government entities and critical infrastructure through 'Dead Glyph Backdoor'. An advisory comprising technical details and mitigation measures is shared below for compliance by all concerned.

2. **Dead Glyph Backdoor**

a. **Gist/Introduction**. Dead Glyph is a 'x64 native binary' and '.Net assembly exploit code' used as an entry method (by hackers) to exploit Windows based operating systems. It is designed to avoid antivirus detection by following processes:

(1) Multistage polymorphic attack strategy.

(2) Random network communication patterns.

b. **Modus Operandi**. Dead Glyph backdoor targets (windows based online systems) through following steps:

(1) **Step-1**. Impersonate/Fake as real windows 'DLL' files having malicious scripts attached.

(2) **Step-2**. Backdoor exploit code then saves fake DLL file in Windows C Drive (Sytems32 Folder).

(3) **Step-3**. The fake DLL file then executes second stage malware by unauthorized issuance of PowerShell scripts.

(4) **Step-4**. Extraction of user's critical data and sharing with attacker using random network communication packet size/ timing pattern to avoid detection.

3. Mitigation Measures. Above in view, following preventive measures are advised:

a. **System/Network Administrator**

(1) Ensure proper system hardening and whitelisting at all levels including OS, BIOS, hardware, software etc (defense in depth).

(2) Install reputed and licensed anti-virus, anti-malware, firewalls, SIEM, SOAR, IPS/IDS, NMS solutions etc.

(3) Regularly manually inspect C Drive System32 folder to check any suspicious file creation activity.

(4) Domain controllers (AD servers) must be regularly monitored for signs of malware infection. Endpoints and network logs should be examined on regular basis to detect anomalous network traffic.

(5) Block outbound network connections from powershell.exe, winword.exe, notepad.exe, explorer.exe, bitsadmin.exe, mshta.exe, excel.exe and eqnedt32.exe.

(6) Windows commands/utilities such as mshta.exe, bitsadmin.exe, finger.exe, certutil.exe, cipher.exe and syskey.exe are not required by the end-users and must be blacklisted for endpoint execution.

(7) Administrators must block execution of all scripts having .vbs, .vbe, .hta, .js, .wsh, .wsf, .com, .pif, .ps1 extensions.

(8) Establish a Sender Policy Framework (SPF) for domain, which is an email validation system designed to prevent spam/malware attachments by detecting email spoofing.

(9) Application whitelisting and strict implementation of Software Restriction Policies (SRP) be ensured to block binaries running from %APPDATA% and %TEMP% paths.

(10) Block attachments of file types: .exe, .pif, .tmp, url, .vb, .vbe, .scr, .reg, .cer, .pst, .cmd, .com, .bat, .dll, .dat, .hip, .hta, .js and .wsf in the emails.

(11) Block execution of above file types (para 4a(9)) in Windows environment as most ransomware/trojan/backdoor samples rely on free execution of these file types.

(12) Regularly Update/patch Microsoft Windows vulnerabilities and other installed software.

(13) Disable RDP of all endpoints (when not required) and patch it against all latest vulnerabilities. Establish site-to-site VPN for remote access/employ zero trust architecture for accessing services.

(14) Centralized monitoring of endpoint Windows logs must be performed to detect anomalous user behavior.

(15) Behavior based malware/anomaly detection be utilized.

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

(17) Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. This data should be kept on a separate system/ storage and backups should be stored offline.

(18) Apply least privileged access across network.

(19) Prioritize authentication and authorization in systems and domains.

(20) Protect data through backups and passwords.

b. **End Users**

(1) Blocking of PowerShell scripts for local users (end users) and only allowed to Admin. To be ensure via privilege and role-based access management.

(2) Keep all software and OS up to date along with timely patching of CVEs.

(3) Install and regularly update reputed antiviruses such as Kaspersky, Avira, Avast etc to scan system regularly.

(4) Do not download attachments from emails or websites unless you are sure about the source/sender.

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

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

(7) Enable multi-factor authentication on all email and banking accounts.

(8) Ensure strong password policy and regularly change passwords.

(9) Do not keep official, secret or private data on online computers.