Subject: **Advisory – Prevention against Weaponized Team Viewer Malicious Exploitation Attempt (Advisory No.12)**

1. **Introduction.** TeamViewer is a popular remote access and desktop-sharing software used all around the globe. Recently, hackers are utilizing it as an attack vector for targeted attacks by sending spear phishing emails with legitimate looking macro documents. Once macro is enabled, the script downloads a malicious version of TeamViewer thus giving hackers full remote access of the system.

2. **Summary of Malicious Attack.** Malware developers have a long history of abusing TeamViewer for delivering backdoors and key loggers. Detail is as under: -

   a. **Attack Vector.** Spear phishing emails with email attachment.

   b. **Mode of Operation.** After user enables the macro code, a legitimate auto hot key AutoHotkey U32.exe program is launched along with AHK script, that contacts the C&C server and further infects the user system.

   c. **Capabilities of Malware.** The AHK scripts have following capabilities:-

      (1) Take screenshots.

      (2) Username and System Information.

      (3) Downloading and executing weaponized TeamViewer.

   d. **Type of Malware**. Macro based Excel Files and Modified TEAMViewer.

   e. **Affected Platform**. Windows OS.

3. **Recommendations**. In order to safeguard against above mentioned form of cyber espionage attempt, following measures are recommended for users and server administrators:-

   a. **For users**

      (1) **Install and update well reputed and trusted antimalware solution** like Kaspersky, AVAST, Avira etc.

      (2) Don't **download and open email attachments from untrusted sources** and forward them to email address **asntisb2@cabinet.gov.pk**

      (3) Download and install software from legitimate website only.

      (4) **Make sure that real time protection of antimalware solution is running along with legitimate Firewall.**

(5) **Always keep windows, softwares and browsers up to date.**

(6) **Don't make use of Internet Explorer or Microsoft Edge for browsing** and utilize well reputed browsers like **Chrome** or **FireFox**.

(7) **Make sure that no other browser extension is installed** except Adblock or Adblock plus and browser is not redirecting to other pages.

(8) **Never enable macros in word or excel documents unless sure about the source.**

b. **For Network / Server / System Administrators.** In order to counter date exfiltration and detecting malware by hostile elements, following steps are recommended for scanning and disinfecting of sensitive date hosting windows base servers.

(1) Start your computer / server in **"Safe Mode with Networking"** mode.

(2) **Terminate known running malicious processes with RKill software** provided by website **bleepingcomputer.com.**

(3) **Remove malicious registry entries** with **RogueKiller** software **hosted at website adlic.com.**

(4) **Remove malware programs from Windows Startup** with **CCLeaner.**

(5) Scan and remove **hidden malicious Rootkits** with **Kaspersky TDSSKiller.**

(6) Run CCleaner **to delete temporary files and folders.**

(7) **Clean adware & unwanted browser toolbars** with **AdwCleaner software** by **M/S Malware Bytes.**

(8) **Remove junkware & Potentially Unwanted Programs (PUP) with JRT (Junk removal tool)** by **M/S Malware Bytes.**

(9) **Remove temporary internet files and invalid registry entries** with **CCleaner.**

(10) **Delete infected Windows Restore Points** and make a new restore point after thorough scan.

(11) **Make sure that host-based firewall and domain Firewall is active on all users of Active Directory.**

(12) Make sure that all softwares installed **have valid digital signatures** by verifying it with legitimate trusted Microsoft utility like **SigCheck**