Subject: **Advisory - Prevention Against Cyber Espionage via Malicious Excel Files (Advisory No. 17)**

1. **Context.** **Malicious excel files** are being used for targeting users via phishing emails. The malicious files are not standard **Excel Spreadsheets** and have **low detection rate** and higher chance of **evading security systems**. The malicious Excel files can also bypass security scanners.

2. **Technical Details**

   a. The malicious excel files are not compiled in standard Microsoft Office Excel, but with a **.NET library** called **EPPlus,** that creates an Office Open XML (00XML) format.

   b. The. **00XML spreadsheet files** lack a section of **compiled VBA code,** specific to Excel documents compiled in Microsoft's proprietary Office software.

   c. The malicious excel files contain a **malicious macro script.** If user opens the Excel files and allows the script to execute (by clicking the **"Enable editing"** button), the macros downloads and installs malware on the user's system.

   d. The payloads of malicious excel files are **info stealer trojans** like **Azorult, AgentTesla, Formbook, Matiex** and **njRat.**

   e. The information stealer trojans dump **passwords from the user's browsers, emails,** and **FTP clients** and send them to C&C servers.

3. **Recommendations**

   a. Install and update licensed and well reputed antiviruses such as Kaspersky, Avira and Avast.

   b. Update all software including **Windows OS**, **Microsoft Office** and **web browsers**.

   c. Do not download attachments from **emails** unless they are from the trusted source.