

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT, CABINET DIVISION  
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
(NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad 16 Sep 2020

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

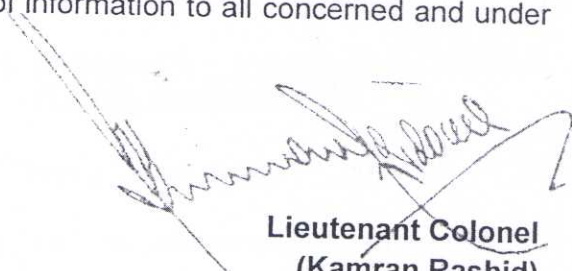
- 21 SEP 2020
- Y(A)  
Y(I.T) ✓  
F.S (Rev. Div)
- The malicious excel files are not compiled in standard Microsoft Office Excel, but with a **.NET library** called **EPPlus**, that creates an Office Open XML (OOXML) format.
  - The **OOXML spreadsheet files** lack a section of **compiled VBA code**, specific to Excel documents compiled in Microsoft's proprietary Office software.
  - 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 download and installs malware on the user's system.
  - The payloads of malicious excel files are **info stealer trojans** like **Azorult, AgentTesla, Formbook, Matiex** and **njRat**.
  - The information stealer trojans dump **passwords from the user's browsers, emails, and FTP clients** and send them to C&C servers.

3. Recommendations

- 165646  
23/9/2020
- Chief (IT)
- Install and update licensed and well reputed antiviruses such as Kaspersky, Avira and Avast.
  - Update all software including **Windows OS, Microsoft Office** and **web browsers**.
- SS(IT) 23/9/20

FBR (FCY) Div No. 165646  
Revenue & Customs Officer's Sectt  
02-1-001-2020

- c. Do not download attachments from **emails** unless they are from the trusted source
4. Forwarded for perusal and dissemination of information to all concerned and under command, please.



**Lieutenant Colonel  
(Kamran Rashid)  
Deputy Secretary (NTISB)  
Ph# 051-9204560**

**All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments**

**Copy to: -**

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-II, Cabinet Division, Islamabad
5. Secretary, NTISB, Cabinet Division, Islamabad
6. Deputy Secretary, NTISB, Cabinet Division, Islamabad
7. Director (IT), Cabinet Division, Islamabad