***IN* INFOSEC ADVISORY – 03/2023**

ZERO DAY VULNERABILITY IN MICROSOFT OFFICE PRODUCTS

1. **Introduction**. Microsoft has identified a phishing campaign conducted by threat actors primarily targeting government entities.

2. **Aim**. The aim of the advisory is to create awareness amongst naval personnel and families regarding the operational methodology of such phishing campaigns, and preventive measures to avoid becoming victims to such malicious activities and divulging personal/ official information.

3. **Applicability and Scope**. The advisory is applicable to all personnel using MS Office applications. The scope covers the attack methodology used by adversaries and steps to be taken to safeguard systems against such exploits.

4. **Methodology Employed by Threat Actors**. The campaign has been tracked to a Russia-based threat actor identified as **Storm-0978**. It involves the exploitation of a MS Office vulnerability which can be executed via malicious word documents which are generally circulated through emails/ social media platforms as various '*topics of interest*'. An adversary can create specifically crafted Microsoft Office documents and convince the victim to open the malicious document which would enable the adversary to execute arbitrary code on the victim's machine. Such 'trojanised' documents create a backdoor for installation of a malicious software known as **RomCom**, which in turn causes breach of data.

5. **Preventive Measures**. The following preventive measures are recommended: -

   (a) Do not open documents received from unverified sources. Only open verified and pertinent attachments received in your inbox.

   (b) Install and update Windows security patches regularly to ensure that all software and firmware are up-to-date.

   (c) Install and regularly update Antivirus software.

   (d) Perform a full Anti-Virus scan on your device at least once a fortnight and delete any malware detected.

6. **Report**. Report any detected cybercrime incident on the national cybercrime reporting portal https://www.cybercrime.gov.in or toll-free helpline number **1930**.