Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 234 **22-02-2024**

Name: Raspberry Robin Malware Exploiting Discord and 0-Day Exploits

Threat Classification: Advanced Malware, Discord Exploitation, 0-Day Vulnerabilities

Affected Software / Services:

- Systems vulnerable to CVE-2023-36802 and CVE-2023-29360

Summary:

Raspberry Robin, previously known as a USB-borne worm, has evolved into a highly sophisticated threat, utilizing undisclosed "0-day" exploits to exploit vulnerabilities before official patches are available. This evolution includes a shift in distribution tactics, with the malware now leveraging Discord for spreading malicious payloads. The malware conceals itself within seemingly harmless archive files downloaded from Discord, exploiting user trust in both a legitimate Microsoft program (OleView.exe) and a malicious DLL with a disguised signature.

Severity	**High**
Attack Vector	Discord Payload Distribution, 0-Day Exploits

Recommendations:

- Prioritize updating systems with the latest security patches, especially for vulnerabilities targeted by Raspberry Robin (CVE-2023-36802 and CVE-2023-29360).
- Conduct thorough training on social engineering tactics, emphasizing the dangers of downloading files from unknown or seemingly trusted sources like Discord.
- Deploy advanced security solutions capable of detecting and neutralizing sophisticated threats beyond traditional antivirus measures.
- Regularly check for active IOCs related to Raspberry Robin and update security protocols accordingly.
- Caution users about the potential risks associated with file downloads from Discord, even within seemingly legitimate conversations.
- Implement robust network monitoring to detect and mitigate lateral movement attempts by Raspberry Robin.
- In case of any incident, please report to this office, through PTA CERT Portal and email.