Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 230 **19-02-2024**

Name: Teams Group Chat Phishing Advisory

Threat Classification: Malware/Phishing

Affected Software / Services:

- Microsoft Teams

Summary:

Cybercriminals are exploiting Microsoft Teams group chat requests to distribute DarkGate malware. Over 1,000 malicious Teams group chat invites were sent, prompting victims to download a file named 'Navigating Future Changes October 2023.pdf.msi.' Once installed, the malware connects to the command-and-control server at hgfdytrywq[.]com. Microsoft Teams' default setting allowing external users to message other tenants is leveraged in this phishing attack.

Severity	**High**
Attack Vector	Teams Phishing

Recommendations:

- Disable External Access in Microsoft Teams unless absolutely necessary for daily business use.
- Train end-users to scrutinize unsolicited messages, even within trusted platforms like Microsoft Teams.
- Consider email as a more secure communication channel when possible.
- Regularly update and monitor security settings in collaboration platforms.
- Ensure that security protocols, including disabling unnecessary features, are implemented in Microsoft Teams to mitigate phishing risks.
- Collaborate with IT security experts to stay informed about emerging threats and best practices.
- If affected, follow incident response procedures, isolate infected systems, and conduct thorough security audits to prevent further damage.
- In case of any incident, please report to this office, through PTA CERT Portal and email.