Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 248 **10-04-2024**

Name: Multi-Stage Malware Attack via Phishing Invoice

Threat Classification: Malware / Phishing

Affected Software / Services:

- All systems susceptible to phishing attacks

Summary:

A sophisticated multi-stage attack campaign leveraging phishing emails disguised as invoices has been detected by cybersecurity researchers. The attack utilizes obfuscation tools such as BatCloak malware and ScrubCrypt to distribute a variety of malware, including XWorm, Remcos RAT, Venom RAT, NanoCore RAT, and a wallet-stealing stealer. The phishing email contains a Scalable Vector Graphics (SVG) file attachment that triggers the attack chain upon interaction, leading to the compromise of targeted systems.

Severity	**Critical**
Attack Vector	Phishing Email

Recommendations:

- Educate users about the risks associated with phishing emails and advise caution when interacting with email attachments.
- Implement robust email filtering and detection mechanisms to identify and block phishing emails before they reach end-users.
- Utilize endpoint protection solutions capable of detecting and mitigating malware infections.
- Ensure all software and systems are regularly updated and patched to address known vulnerabilities exploited by malware.
- Monitor network traffic for suspicious activity indicative of a compromise and deploy advanced threat detection solutions.
- Enhance incident response capabilities with advanced threat detection and response solutions to improve threat visibility and response times.
- In case of any incident, please report to this office, through PTA CERT Portal and email.