Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 225 **2-2-2024**

Name: Fabookie Trojan Targeting Facebook Accounts

Threat Classification: Malware

Affected Software / Services:

- All platforms and operating systems susceptible to the Fabookie Trojan

Summary:

Fabookie is a Trojan specifically designed to target Facebook accounts, stealthily infiltrating computer systems to harvest sensitive information, including usernames and passwords. Operating discreetly in the background, Fabookie remains undetected for extended periods, enabling unauthorized access to Facebook accounts, leading to potential identity theft or compromised accounts sold on underground markets. Users may only become aware of the attack when they notice suspicious activity or unauthorized access on their Facebook accounts. Based on general practices of trojan deployment, it could utilize various deceptive means for installment, such as Phishing Links, Malicious Downloads, Email Attachments etc.

Severity	**High**
Attack Vector	Social Engineering / Phishing

Active IOCs

Domain Name
app[.]alie3ksgaa[.]com
ji[.]alie3ksgdd[.]com

MD5
67a7cd9f9fef32fc81696237166d8359
d7c215d443e28dc0fe78c36909d1356a
bfa5bf4c04cd22e68df0f443effca797
e9fdeb5c84d1876d82cc117fde5f0879
13e50553cf74404e0667de093b05d4bb
SHA-1
28c8e9288ec2c3a84a48312c8bac4fec0623205a
d2b4e780b13305b25cba7cd3b2259d94d84120a8
eceedf94f82d252f20ad8eb3dd64fcb9a6c09495
89f2da007b8f763414579b819ba0eed9caeb1521
be6db70542a1a4ef925613d8553d28e54a52f423
SHA-256
af96622e503cea942a82577fe25a1284111cb3614a29aaaefaf393c059409008
8f1db790b8dcd0cfa72966ee8702bfd44c52600a290e40285b21bd6f356c12c5
d9cba8aea678e19b497b36f3d5f9869dbd042e45759039444581a5234c59ee7f
0f737197c5a1b9b736028c7fd377d0ecce5ca0dc56daef3348d8fe990f286258
718643fa7796ed792faa9cc2a139a0d566dae24b00dbd5d7019386d394f79436

Recommendations:

- Utilize controls to block all IoCs and investigate potential compromises in environment.
- Enhance account security with 2FA to prevent unauthorized access, even with stolen credentials.
- Safeguard critical data by routinely backing up important information.
- Be cautious with emails, attachments, and links from unknown sources. Avoid downloading software or clicking on suspicious content.
- Prevent vulnerabilities by ensuring all software, including the OS, is up-to-date with the latest security patches.
- Maintain secure offline backups of critical data, including Facebook Business account information, for swift recovery in case of an attack or data loss.
- In case of any incident, please report to this office, through PTA CERT Portal and email.