Cyber Crime Information – 151

April 21st, 2022

Subject: Banking Trojans (Malware) stealing confidential information to defraud citizens

Threat Summary

A banker Trojan is a piece of malware that steals banking credentials from citizens who use internet/mobile banking services through apps or websites. Recently a multitude of cases related to such Trojans, e.g., Sharkbot, Escobar, Zbot, Trickbot, etc. have been observed. Banking Trojans are disguised as innocent applications/webpages, and avoid being detected by "having dormant capabilities, hiding components in other files, forming part of a rootkit, or using heavy obfuscation." Predominantly victims' devices are infected through e-mail attachments (or e-mail links), drive-by downloads, deceptive pop-up windows, etc.

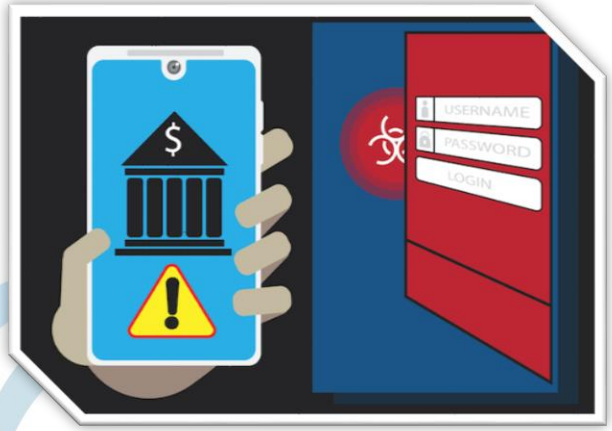

Fig. 01 – Banking Trojans defrauding citizens

Modus Operandi

- Cybercriminals mask malicious apps under the guise of legitimate applications (mobile banking and payment apps are targeted generally), which can often be downloaded from official app stores.
- Banking malware (hidden in malicious apps) create a backdoor, allowing fraudsters to gain access to the victim's device, or it may instead copy a bank client's credentials by spoofing a financial institution's login webpage.
- When the victim accesses his/her online banking account, the domain is specified in the configuration file downloaded by the malware from the malicious servers controlled by the hackers.
- The malware sends a request to the malicious servers controlled by cybercriminals and lets them know the user is trying to access the domain specified in the configuration file.
- The malicious server specifies a page on the online banking account – usually the login page – where the attack occurs.

- When the user accesses the specified page, the malware sends a request to the malicious server, sending back a modified page into the user's browser. The modified page tricks the user into believing that he is entering his credentials in the normal page of the online banking account.
- The modified page asks for the user's sensitive information, such as credentials for the online banking websites / credit / debit card number / pins, etc.
- The main goal of the trojan is to steal enough information to allow the threat actors to take over victims' bank accounts, siphon available balances, and perform unauthorized transactions.

Suggestions

- Avoid downloading software from unofficial sources. Remove non-essential applications.
- Always use Two-factor authentication/MFA and all the security features provided by the banks.
- Do not open e-mails or attachments from unknown individuals. Do not communicate with unsolicited e-mail senders.
- Ensure operating systems and applications are updated to the most current versions.
- Deploy a traffic filtering solution that can spot even hidden threats and suspicious log of network traffic.
- Update anti-malware and anti-virus software and conduct regular network scans.
- Report any such incidents on the ***cybercrime.gov.in*** portal and follow ***@CyberDost*** on Twitter, YouTube, Facebook, Instagram, Public, Koo and LinkedIn to know more about safety tips.

Regards,

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207