Malicious Software Cerberus

drishtiias.com/printpdf/malicious-software-cerberus

Why in News

Central Bureau of Investigation (CBI)malicious software (cerberus) threat Covid-19 Recently, the has sent alerts to all the States, Union Territories and the central agencies on a that is taking advantage of the pandemic.

> **cyber alertCerberusInterpol**The related to has been sent on the basis of inputs received from the .

Key Points

- **Cerberus: Banking Trojan.** It is a It is primarily used to steal financial data, such as credit card numbers.
- **Trojan:**
  - Trojan is a type of malicious code or software to damage, disrupt, steal, or inflict harmful action on data or network.
  - **overlay attacks to trick victims two-factor authentication**
    - **Overlay attacks: (E.g. login credentials or bank card numbers),** An overlay attack happens when an attacker places a window over a legitimate application on the device. When the target application is running, the overlay opens messages or data input forms identical to the real ones. Victims enter information believing that they are dealing with the original program.
    - **Two-factor authentication:** It is a two step verification security process in which users go through two authentication processes to verify themselves.
    The Trojan can also use into providing personal information and can capture details.
  - **Banking Trojan** is a malicious program used in an attempt to obtain confidential information about customers and clients using online banking and payment systems.

- **Working of Cerberus**
  - **sends SMS**It takes advantage of the Covid-19 pandemic and to lure a user to download the link containing the malicious software.
  - **phishing campaigns**It deploys its malicious application usually spread via to trick users into installing it on their smartphones.
  - **Phishing:**

    The link takes to a fake website and once details like login name and passwords are entered, the login credentials reach the hacker.

    The email or text message carrying a link appears to come from a trusted source like a bank.

Source:TH