1. ModifiedElephant – a hacking group

Prelims Syllabus: Information Technology

Mains Syllabus: GS-III Awareness in the fields of IT, Space, Computers, Robotics, Nano technology, Bio-Technology and Issues Relating to Intellectual Property Rights.

Why in News?

- It was recently found by an American Agency that ModifiedElephant, a hacking group, had allegedly planted incriminating evidence on the personal devices of Indian journalists, Human Rights Activists, Human Rights Defenders, Academics and Lawyers.

What is ModifiedElephant? What's the Issue?

- ModifiedElephant operators have been infecting their targets using spearphishing emails with malicious file attachments.
- Spearphishing refers to the practice of sending emails to targets that look like they are coming from a trusted source to either reveal important information or install different kinds of malware on their Computer Systems.

How does it Work?

- Through mail, the group delivers malware to their targets.
- NetWire and DarkComet, two publicly-available remote access trojans (RATs), were the primary malware families deployed by ModifiedElephant.
- It also sent android malware to its victims.

What's the Difference between Malware, Trojan, Virus, and Worm?

- Malware is defined as a software designed to perform an unwanted illegal act via the computer network. It could be also defined as software with malicious intent.
- Malware can be classified based on how they get executed, how they spread, and/or what they do. Some of them are discussed below.
- **Virus:** A program that can infect other programs by modifying them to include a possible evolved copy of itself.
- **Worms:** Disseminated through computer networks, unlike viruses, computer worms are malicious programs that copy themselves from system to system, rather than infiltrating Legitimate Files.
- **Trojans:** Trojan or Trojan horse is a program that generally impairs the security of a system. Trojans are used to create back-doors (a program that allows outside access into a

secure network) on computers belonging to a secure network so that a hacker can have access to the secure network.

- **Hoax:** An e-mail that warns the user of a certain system that is harming the computer. The message thereafter instructs the user to run a procedure (most often in the form of a download) to correct the harming system. When this program is run, it invades the system and deletes an important file.
- **Spyware:** Invades a computer and, as its name implies, monitors a user's activities without consent. Spywares are usually forwarded through unsuspecting e-mails with bonafide e-mail i.ds. Spyware continues to infect millions of computers globally.