ModifiedElephant

February 14, 2022

In news– American cybersecurity firm SentinelOne has released a report on a hacking group called ModifiedElephant, recently.

About ModifiedElephant-

- It is a **hacking group that typically weaponises malicious Microsoft Office files to deliver malware** to their targets.
- **Its operators have been infecting their targets using spear phishing emails** with malicious file attachments over the last decade, with their techniques getting more sophisticated over time.
- Its purpose is to **obtain remote access to and unrestricted control of victims' devices.**
- The report also revealed that **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** which is an unidentified commodity trojan delivered as an APK file.
- The analysis revealed that the **group operates in an overcrowded target space where multiple actors are targeting the same victims** and that it may have relations with other regional threat actors.
- As per report, **Multiple individuals targeted by ModifiedElephant have also been targeted by Pegasus** and other mobile surveillance spyware.
- ModifiedElephant's **phishing email payloads share infrastructure overlaps with Operation Hangover, an espionage network** previously used in surveillance efforts against targets of interest to Indian national security.
- In India, it allegedly planted incriminating evidence on the personal devices of Indian journalists, human rights

activists, human rights defenders, academics and lawyers including the activists arrested in the Bhima Koregaon ase of 2018.

- **Devices can be protected from this malware with multi-factor authentication (MFA) t**o ensure that ones' email IDs and other accounts aren't compromised in the first place.
- With MFA, one needs two pieces of information, like a password and a randomly generated token, in order to log in to a system or account.

What is NetWire?

- It is a RAT **focused on password stealing, keylogging and remote control** capabilities.
- It has been **in use since 2012 and was typically distributed through social engineering campaigns.**
- Its distribution as a second payload using Microsoft Word documents is a fairly recent phenomenon.

What is DarkComet?

- It is another RAT that can take **control of a user's system using a convenient graphical user interface**.
- It was **initially developed in 2008 by French infosec programmer Jean-Pierre Lesueur** and can be used to spy on victims using screen captures, key-logging, or password stealing.

What is Spear Phishing?

It 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.