# India Ransomware Report 2022 by CERT-In

April 19, 2023

**In news–** India's national cyber agency CERT-In has

**Key highlights of the report-**

- **India saw a 53 per cent increase in ransomware incidents in 2022** (year-over-year) and **IT and ITeS was the majorly impacted sector followed by finance and manufacturing**.
- Ransomware players targeted critical infrastructure organisations and disrupted critical services in order to pressurise and extract ransom payments in 2022.
- **Variant wise, Lockbit was a majorly seen variant in the Indian context followed by Makop and DJVU/Stop ransomware.**
- Many **new variants** were observed in **2022 such as Vice society, BlueSky** etc.
- In 2022, a massive ransomware attack disrupted the systems at the All India Institute of Medical Science (AIIMS), crippling its centralised records and other hospital services.
- According to the CERT-In report, at the large **enterprise level, Lockbit, Hive and ALPHV/BlackCat, Black Basta variants became major threats**, whereas Conti, which was very active in the year 2021, became extinct in the first half of the year 2022.
- Makop and Phobos ransomware families mainly targeted medium and small organisations.
- At individual level, Djvu/Stop variants continued dominance in attacks over the past few years.
- Most of the ransomware groups are exploiting known vulnerabilities for which patches are available.
- Some of the product wise vulnerabilities being exploited are in tech companies like Microsoft, Citrix, Fortinet,

SonicWall, Sophos, Zoho. and Palo Alto etc.

- Ransomware gangs are commonly using Microsoft Sysinternals utilities such as PsExec for lateral movements.
- On an average, the restoration time is about 10 days for infections in reasonably large infrastructure networks.