

Ransomware Trends in 2024

Why in News?

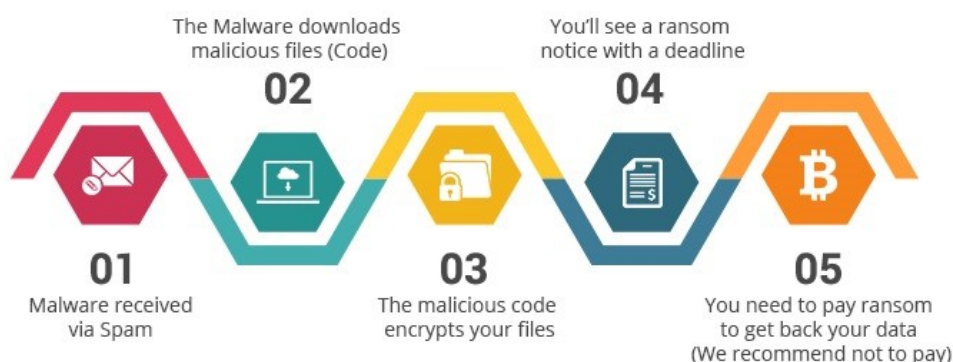
Recently, the CyberPeace released a report of *Ransomware Trends 2024: Insights for Global Cybersecurity Readiness*.

- CyberPeace used advanced Open Source Intelligence Techniques (OSINT), for continuous monitoring of Ransomware Group activities.

Ransomware

- It is a type of malware that holds data and devices hostage until a ransom is paid.
- **Encrypting ransomware** - Holds the victim's data hostage by encrypting it.
- **Non-encrypting ransomware** - Locks the victim's entire device, usually by blocking access to the operating system.

How Ransomware Works

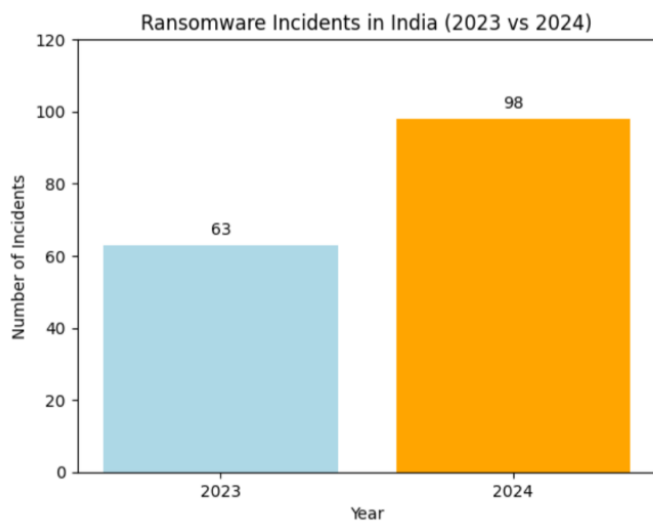


- **Threat** - Ransomware groups orchestrated 5,233 claims across 153 countries using these underground resources.
- **Most targeted nations** - United States, followed by Canada, the UK, Germany, and others.
- It revealed that killsec was the most frequent threat, followed by lockbit3 as the second most prominent threat.
- **Vulnerable targets** - It poses significant risks to industries, governments, and individuals alike.
- **In India** - It witnessed a 55% rise in ransomware attacks with 98 recorded cases.
- The industrial sector was frequently targeted, accounting for 75% of the total incidents.
- The government sector experienced the least impact, with only 3% of the incidents, indicating minimal targeting compared to the other sectors.

Impacted Sectors in India

Incidents

Industrial sector	75%
Health Care center	12%
Finance sector	10%
Government sector	3%



- **Proactive Measures** - Implement Data Backup and Recovery Plans
 - Enhance Employee Awareness and Training
 - Adopt Multi-Factor Authentication (MFA)
 - Utilize Advanced Threat Detection Tools
 - Conduct Regular Vulnerability Assessments.

References

1. [The Indian Express| Impact of Ransomware Attacks in India](#)
2. [CyberPeace| Ransomware Trends 2024](#)

Related News

[Increasing Ransomware Attacks in India](#) | [Ransomware attacks on Indian IT Firms](#)