Energy sector turns prime target for cyber attacks: Seqrite-DSCI report

Hyderabad

The power and energy sector has become a prime target for cybercriminals, accounting for 29 per cent of all malware detections in 2024, according to a report by cybersecurity solutions company Seqrite.

Over 15,000 malware detections were recorded across 2,132 endpoints in the sector, indicating a high level of targeted attacks. This translates to an average of seven detections per endpoint, highlighting the persistent and sophisticated nature of these threats.

"This alarming statistic highlights the sector's vulnerability and its attractiveness to threat actors seeking to compromise critical national infrastructure," the report, which was jointly prepared with the Data Security Council of India (DSCI), said.

The most prevalent malware identified in the sector was LNK.RaspRobin.48713, a particularly insidious threat that spreads via malicious shortcut (.lnk) files on removable media such as USB drives.

"This malware establishes connections to external servers, enabling it to download additional malicious payloads and establish persistence on infected systems," it said.

The prevalence of malware in the power and energy sector is especially concerning due to its propagation method. The use of removable media as an attack vector poses a significant risk in operational environments where USB drives are commonly used to transfer data between air-gapped systems.

How to stay safe?

To stay safe, organisations in this sector must implement advanced endpoint detection and response (EDR) solutions, conduct regular cybersecurity awareness training for employees, and develop robust incident response plans.

"Strict policies should be enforced regarding the use of removable media, and network segmentation should be implemented to isolate critical systems from potentially compromised networks," the repot said.