



## Tamil Nadu Manufacturing Belt Sees a Steep Rise in Malware Infections in 2025, Reveals Seqrite

Tamil Nadu's manufacturing belt has long been the engine driving India's industrial growth. But beneath the vast network of automotive assembly lines, engineering workshops, and precision fabrication units, malware infections are quietly infiltrated factories, design floors, and supply chains, turning trusted systems into unwitting accomplices for cybercriminals. Findings from [India Cyber Threat Report 2026](#) by [Seqrite](#), the enterprise security arm of [Quick Heal Technologies Limited](#), a global provider of cybersecurity solutions, shine a spotlight on this vulnerability.

Drawing from unified telemetry across more than 8 million endpoints, the report reveals that Tamil Nadu recorded 7.51 million malware detections between October 2024 and September 2025, placing it seventh among India's most targeted states. Chennai, the state's industrial nerve centre, clocked 4.27 million detections, ranking ninth among India's top affected cities. Malware families with modular loaders that disable protections and deploy ransomware were found to be rampant, exploiting unpatched endpoints in production environments. Cryptojacking variants such as Nsis.Bitmin quietly hijacked compute resources, while infectors propagated laterally across networked machinery.

Beyond just stealing data, these infections halt assembly lines, corrupt blueprints, and expose intellectual property to extortion. Design files, production schedules, supplier credentials, and employee records flow freely across endpoints, servers, and third-party portals. A single infected USB on the shop floor can cascade into a network-wide breach. Legacy systems running outdated Windows evade modern defenses, while remote access tools for vendor coordination open backdoors. And as factories digitize with IoT sensors and AI-driven quality control, the attack surface explodes.

For Tamil Nadu manufacturers, this translates to downtime risks that no business can afford, especially when ransomware peaked at 185 incidents in January 2025, often post-compromise from initial malware infections that caused data breach. Blueprints, employees' personal information, supplier lists, etc. vanished into the dark web, becoming fodder for potential scams. The Digital Personal Data Protection (DPDP) Act, 2023, aims to prevent this through lawful processing of data, purpose limitation, and immediate breach reporting, with penalties up to ₹250 crore for lapses.

The alarming nature of these findings makes deploying advanced, enterprise-grade cybersecurity solutions an absolute necessity. Tailored for data-intensive industries like manufacturing, all Seqrite products are fully compliant with the DPDP Act, empowering manufacturers in Tamil Nadu and beyond to secure their operations while meeting legal obligations. Coupled with Seqrite Threat Intelligence, Ransomware Recovery as a Service (RRaaS), and AntiFraud.AI, these solutions provide the predictive defense needed to stay ahead of cognitive threats forecasted for 2026.