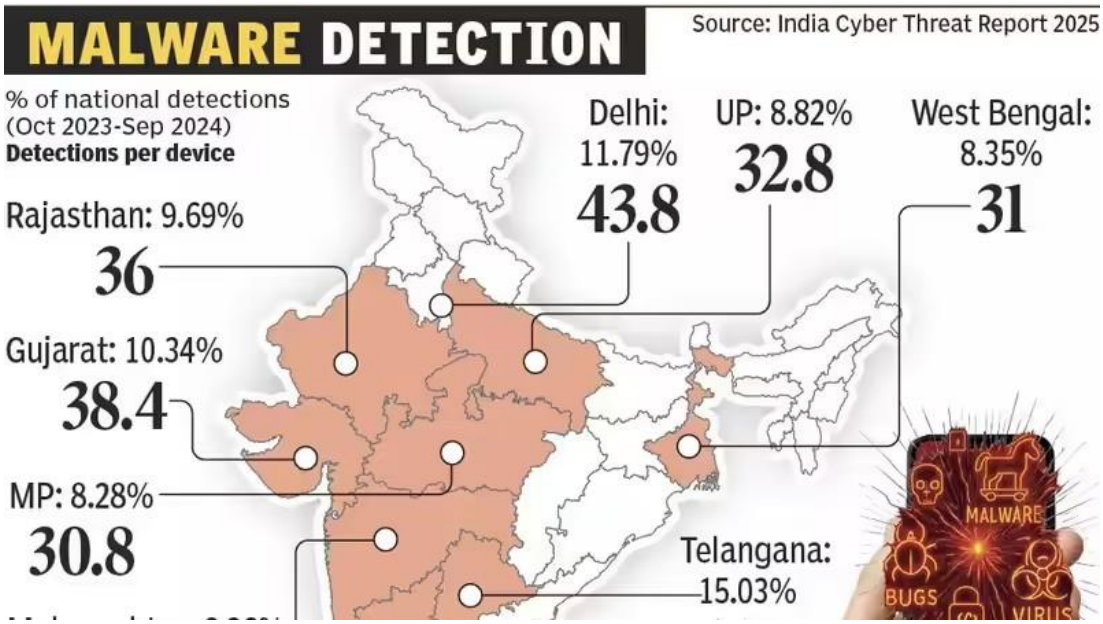
38 LAKH MALWARE HITS IN GUJARAT. IS YOUR DEVICE SAFE?

Think Viruses, Trojans, Spyware. These Are Malware In Action— Stealing Data & Hijacking Systems. Gujarat Is India's Fourth- Most Attacked State With 38L Cases In Just A Year, Reveals India Cyber Threat Report 2025.



Think Viruses, Trojans, Spyware. These Are Malware In Action— Stealing Data & Hijacking Systems. Gujarat Is India's Fourth-Most Attacked State With 38L Cases In Just A Year, Reveals India Cyber Threat Report 2025. Read on

There is an invisible war happening right now, and most people in Gujarat don't even know they are in it. While you were checking your emails this morning, roughly 702 malware attacks were launched somewhere in India. By the time you finish reading this sentence, another dozen devices will have been infected.

And Gujarat is taking some of the heaviest hits. According to the India Cyber Threat Report 2025, released by the Data Security Council of India (DSCI), the state is the fourth-most attacked region in the country, with 38.15 lakh malware detections recorded in a single year.

The study tracked 8.44 million devices nationwide that had Seqrite/Quick Heal antivirus installed. In Gujarat, the detection rate hit 38.44% — meaning that out of every 100 monitored devices in the state, 38 encountered at least one malware threat during the year. Put differently: pick any three devices in Gujarat with this antivirus — laptops, phones, desktops, tablets — and one of them has likely already been attacked.

The numbers come from telemetry data analyzed by Seqrite Labs between Oct 2023 and Sep 2024. Those devices reported 369.01 million malware incidents nationwide. The data reveals that 51.13% of the total national security detections are concentrated across just 10 states.

Malware comes in many forms: viruses, spyware, trojans, ransomware, worms — an entire arsenal of malicious software designed to damage devices, steal information, hijack networks or hold your data hostage until you pay up. And the attacks are not random. They are strategic.

Gujarat's high detection rate stands out, even among the most affected states in the country. The report points to two specific factors behind this: industrial exposure and manufacturing sector vulnerabilities. These sectors often deal with outdated systems and large-scale digital infrastructure handling mountains of sensitive data. To a cybercriminal, that is a goldmine.

Manufacturing accounts for nearly 7% of the total malware detections across India. And at 38.4%, Gujarat, one of the country's industrial powerhouses, is absorbing a disproportionate share of that heat. Compare that to other states. Telangana leads with 55.90 detections per endpoint (device) (15.03% of national detections). Tamil Nadu follows with 44.54 per endpoint (11.97%). Delhi sits at

43.86 per endpoint (11.79%). These are tech-heavy states with advanced security

infrastructure — which also makes them prime targets.

THE AI ARMS RACE

The threats in 2025 aren't the same ones from even two years ago. Artificial intelligence has entered the scene and upended everything. AI is now powering the biggest cyber threats: scams where your boss asks you to transfer money, deepfake videos and audio impersonating executives, ransomware that learns from your behaviour and adapts in real time. The attacks are getting harder to detect and even harder to stop.

Between 2021 and 2024, cyber threats detected using behavioural-based methods skyrocketed from 5 million to over 53 million — a 960% increase.

Old-school antivirus works like a bouncer with a blacklist — if your face isn't on it, you're in. That's signature-based detection. Behaviour-based detection watches how you act: a program suddenly accessing multiple files, or logins from Mumbai, New York, and London within an hour. That's not normal. "Cybercriminals have gotten smarter," says Manish Thakar, a cybersecurity expert. "They use polymorphic malware that constantly changes code, hide inside normal system tools, or attack without leaving files behind — easily fooling older security tools." Among malware types — viruses, trojans, ransomware, worms — spyware poses a particularly insidious danger.

A senior official at National Forensic Science University explains that modern spyware goes beyond stealing keystrokes and screenshots. "Advanced variants can self-replicate like worms, encrypt files for ransom, or hijack computing power for cryptomining," he says. Mobile spyware disguises itself within legitimate-looking apps, games, or utilities — this is why Google Play Store regularly purges suspicious applications. Zero-day exploits and advanced persistent threats that hide for months require faster, smarter defences.