India Leads Global Mobile Malware Attacks, IoT Threats Escalate: Finds Zscaler ThreatLabz 2025 Report

Key Findings:

- India continues to be the top target for mobile attacks, with 26% of activity
- The US remains the top target for IoT attacks, with 54% of activity, while India ranked fourth with 5%

New Delhi, January 12, 2026 – Zscaler, Inc., the leader in cloud security, today published the India findings from its Zscaler ThreatLabz 2025 Mobile, IoT, and OT Threat Report, outlining how threat actors are leveraging malware attacks and constantly evolving their tactics. The report uncovered hundreds of malicious apps in the Google Play Store that have been downloaded over 40 million times, targeting users that are searching for productivity and workflow apps. Based on Zscaler's mobile telemetry dataset, the ThreatLabz team identified several emerging mobile threats and new malicious activity, providing valuable insights to help enterprises stay ahead of attackers in a mobile-first world.

Hundreds of malicious apps downloaded over 40 million times

Similar to last year, this year we again saw threat actors developing and releasing malicious applications targeting trusted marketplaces and hybrid work environments. The result, which the report reveals is a 67% year-over-year increase in Android malware transactions, reflects the continued risks of spyware and banking malware. ThreatLabz researchers identified 239 such applications hosted on the Google Play Store, which were collectively downloaded 42 million times.

A key distribution channel for this malware was the "Tools" category, disguising malicious applications as productivity and workflow tools. This tactic capitalizes on users' trust in functionality-driven applications–a trust that is particularly strong in hybrid and remote work settings where mobile devices are integral to professional tasks.

Retail and Hospitality remain top target for mobile and IoT attacks

ThreatLabz's analysis of India telemetry reveals that Retail & Wholesale (38%) and Hospitality, Restaurants and Leisure (31%) as the most frequently targeted verticals, followed by Manufacturing (16%) and Energy, Utilities, Oil & Gas (8%). The concentration in consumer-facing and operations-heavy environments underscores attackers focus on high-transaction, high-dependency IoT deployments.

Most prevalent IoT malware families in India

Backdoor and botnet style malware families dominated detections. IoT.Backdoor.Gen.LZ was the most prevalent with 85% of observed cases, followed by ABRisk.IOTX 0 (8%) and IoT.Exploit.CVE 2020 8195 (1%).

Mobile attacks cluster in India, US and Canada; US is the IoT threat epicenter at 54 percent

Worldwide, mobile threats have surged, with the majority of these attacks concentrated in three key regions: India, accounting for 26% of all mobile attacks, the United States at 15%, and Canada at 14%. India, in particular, experienced a significant 38% increase in mobile threat attacks compared to the previous year.

The top five countries that receive the most mobile malware traffic are:

- India (26%)
- United States (15%)
- Canada (14%)
- Mexico (5%)
- South Africa (4%)

“India’s challenge is stark with breakneck digitization across UPI, super apps, and a sprawling IoT estate, making the country a high-value target,” said **Suvabrata Sinha, CISO in Residence, Zscaler**. “The way forward for security leaders is to operationalize Zero Trust end-to-end, put identity- and device-centric access in front of users, apps, and OT; continuously inspect encrypted traffic to expose phishing and embed mobile threat defense into enterprise policy and extend these controls to branch, OT, and cellular IoT so attackers have nowhere to hide.”

The report also revealed that the US is both a hub for IoT activity (54.1%) and a primary target for malware attacks. The top five countries that receive the most IoT malware traffic are:

- United States (54%)
- Hong Kong (15%)
- Germany (6%)
- India (5%)
- China (4%)

“Attackers are pivoting to areas with maximum impact. We’re seeing a YoY rise of 67% in malware targeting mobile devices and 387% in IoT/OT attacks on energy sectors often hosting critical infrastructure, which is a massive swing,” said **Deepen Desai, EVP and Chief Security Officer at Zscaler**. “A Zero Trust everywhere approach, combined with AI-powered threat detection, is imperative to reducing the

attack surface, limit lateral movement, and provide organizations the defense they need against ever-evolving attacks."

Additional highlights and new findings this year

- A new backdoor called Android Void malware has infected 1.6 million Android-based TV boxes, primarily in India and Brazil
- New Remote Access Trojan (RAT), Xnotice, was identified for targeting job seekers in the oil and gas industry, particularly in MENA
- Adware overtook the Joker malware family as the top mobile threat, with a leading 69% of cases, while Joker dropped to 23% of cases, from 38% last year
- Threat actors are abandoning card-focused fraud in favor of mobile payments

Defending against growing IoT, OT and Mobile threats

Zscaler Zero Trust Branch delivers comprehensive security and operational efficiency for branch offices, remote sites, and distributed networks, designed for environments that rely heavily on mobile, IoT, cellular IoT, and OT technologies. Using a cloud-native and AI-driven Zero Trust architecture, Zscaler aims to ensure all users, devices, and applications are safeguarded with continuous real-time verification and robust policy enforcement, regardless of their location relative to the traditional network perimeter.

Zscaler Cellular offers secure, scalable, and efficient connectivity as a service for IoT and mobile devices that rely on cellular connections. This solution, powered by the Zscaler Zero Trust Exchange™ platform, addresses the growing security challenges posed by billions of IoT devices and mobile endpoints, which traditional security methods often fail to secure effectively. It achieves this by enforcing granular policies, providing centralized visibility, and eliminating attack surfaces for all cellular traffic.

Research Methodology

Mobile

The research methodology for this report includes analysis of mobile transactions and associated cyberthreats based on data collected from the Zscaler cloud between June 2024 and May 2025. The dataset comprises more than 20 million threat-related mobile transactions.

IoT/OT

The team focused their research on understanding the distinct attributes and activity of IoT devices via device fingerprinting (DFP) and analyzing the IoT malware threat landscape.

Device fingerprinting data from March 2025 to May 2025 included:

- A complete inventory of devices, including device types and manufacturers
- The volume and source of IoT device transactions
- The industries and geographies contributing to IoT traffic

IoT malware threat data from June 2024 to May 2025 included:

- The most active malware families
- The industries and geographies most targeted by IoT attacks
- The top attacked devices

About Zscaler

Zscaler accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centers globally, the SASE-based Zero Trust Exchange is the world's largest in-line cloud security platform.