Trend Micro's Midyear Report reveals India's cybersecurity challenges

Dais World | 15/10/2024 03:31 PM

India ranks among the top targets for email, ransomware and malware attacks putting key industries at risk

- *India ranks 2 globally in email threats, accounting for 8.3% of total detections by Trend Micro*
- *India ranks 3 globally for malware detection, contributing 4.7% to the total threats identified by Trend Micro*
- *Banking sector hit hardest by Malware and Ransomware attacks followed by Government and Manufacturing in the first half of 2024*

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, recently unveiled its highly anticipated Trend Micro 2024 Midyear Cybersecurity Threat Report outlining India's heightened cybersecurity risks.

The report underscores India's growing prominence as a prime target for sophisticated cyberattacks, such as email threats, ransomware and malware. With the nation's digital infrastructure rapidly expanding across critical sectors like Banking, Government, and Manufacturing, India now stands at the forefront of global cybersecurity challenges. The findings reveal an urgent need for organisations to strengthen their defences against evolving cyber threats.

Ransomware and Malware Surge

While Japan and The United States currently lead the world in malware detections, India ranks third worldwide with 4.7% of all detected threats. Regionally, India holds the 2 spot in Asia, responsible for 9.95% of malware cases, and dominates South Asia with a staggering 94.2% of all

malware detections highlighting its increasing vulnerability in this area. Notable malware families like CoinMiner, fakeMS, and Mudyupdate present severe risks to the nation's critical sectors.

On the ransomware front, India ranks 10 globally and 6 in Asia, with 1,17,200 ransomware threats detected in 2024—accounting for 2.95% of global and 4.97% of Asia's ransomware incidents. In South Asia, India leads with 73.8% of ransomware cases, making it a dominant target. Key ransomware families such as WCry, Cobra, and GandCrab repeatedly attack critical industries like Banking, Government, and Manufacturing, which remain lucrative targets for financially driven ransomware gangs.

Escalating Email Threats in the region

India grapples with a surge in email-based attacks, ranking 2 globally, behind the United States and leading the charge in Asia. Out of 1,018 billion email threats worldwide, India accounted for an alarming 8.3%, translating to 84.17 million threats. Dominating South Asia, India is responsible for 92.27% of the region's email-based incidents, underscoring the critical need for organisations to prioritise robust email security solutions to defend against this rising menace.

*Commenting on the report's findings, **Sharda Tickoo, Country Manager for India & SAARC**, Trend Micro said, "As cybercriminals employ increasingly sophisticated tactics, key sectors in the region are increasingly under attack from ransomware, email threats, and malware. Staying ahead requires a proactive, unified platform approach rather than fragmented solutions. Our report provides strategic insights for businesses to strengthen their defenses, especially as emerging technologies like generative AI transform the threat landscape. The time to shift from reactive to proactive cybersecurity is now, with a focus on comprehensive threat detection and heightened awareness."*

Furthermore, the report indicates that globally, cloud-based apps, services, and assets are at heightened risk as cybercriminals are exploiting exposed credentials and vulnerabilities. The lack of updated endpoint protection on unmanaged devices further exposes businesses to significant risks. Additionally, cybercriminals have capitalsed on the growing interest in AI technologies by employing tactics such as jailbreaking existing LLMs, bundling legitimate AI software with malicious payloads, and utilising deep fake-generating AI tools.

Trend Micro, dedicated to empowering organisations and individuals with advanced cybersecurity solutions to combat evolving threats in today's digital landscape, advises security leaders to:

1. *Implement measures to prevent threats from infiltrating networks, proactively anticipating ransomware attacks that could lead to extortion after data breaches*
2. *Transition from isolated security tools to a unified platform approach that integrates seamlessly, enhancing overall security posture*
3. *Recognise that AI capabilities can not only streamline operations but also serve legitimate security purposes against cybercriminals exploiting the same technologies*
4. *Conduct training programs to educate end users on identifying and avoiding risky websites and links, as human error remains a critical vulnerability*
5. *Prioritise the efficiency of Security Operations Centers (SOCs) by closely monitoring cloud applications as they become integral to daily operations*
6. *Collaborate with reliable security vendors that utilise a platform-based approach, ensuring resources are secured and continuously monitored for vulnerabilities*

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fuelled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's AI-powered cybersecurity platform protects hundreds of thousands of organisations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, Trend's platform delivers a powerful range of advanced threat defence techniques optimised for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 70 countries, Trend Micro enables organisations to simplify and secure their connected world.

Reach out to us at PR Desk

Read more on our Partner sites: Growth Reports Business | The Progress Catalyst

Get rewarded for your reading habits on the Dais World app!