ET Government
Your Exclusive e-Governance Source

India Cyber Threat Report 2025 by Seqrite spots 369 mn malware detections across 8.44 mn installations

The report also offers a state-wise analysis of malware detections, pinpointing Telangana, Tamil Nadu, and Delhi as the most affected regions. It also sheds light on industry-specific vulnerabilities, identifying BFSI, Healthcare and Hospitality as the sectors most targeted by cybercriminals.

Online Desk · ETGovernment
Updated On Dec 5, 2024 at 06:53 PM IST

The report breaks down malware subcategories, with Trojans leading at 43.38% of detections, followed by Infectors at 34.23%.

NEW DELHI: Seqrite, the enterprise arm of global cybersecurity solutions provider, Quick Heal Technologies, has unveiled its latest cybersecurity initiatives at the 19th nasscom-DSCI Annual Information Security Summit (AISS) 2025, aimed at fortifying India's digital infrastructure against evolving cyber threats.

The centerpiece of Seqrite's announcements was the 'India Cyber Threat Report 2025', a comprehensive study conducted in collaboration with the Data Security Council of India (DSCI). This report provides an in-depth analysis of the current cybersecurity landscape in India, revealing alarming statistics and trends. The study identified a staggering 369 million malware detections across an installation base of 8.44 million in India, highlighting the scale and intensity of cyber threats facing the nation. Notably, 85.44% of detections relied on signature-based methods, while 14.56% came through behavior-based detection, emphasizing the need for adaptive security measures.

The report breaks down malware subcategories, with Trojans leading at 43.38% of detections, followed by Infectors at 34.23%. The Android-based security detections reveal a concerning distribution of threats, wherein malware accounted for 42% of all detections, followed by Potentially Unwanted Programs (PUPs) as the second most common threat at 32%. Adware comprised 26% of detections in Android devices. The report also offers a state-wise analysis of malware detections, pinpointing Telangana, Tamil Nadu, and Delhi as the most affected regions. Furthermore, it sheds light on industry-specific vulnerabilities, identifying BFSI, Healthcare and Hospitality as the sectors most targeted by cybercriminals.

Alongside the 'India Cyber Threat Report 2025', the company introduced its cutting-edge Seqrite Malware Analysis Platform (SMAP). This advanced tool is designed to empower security professionals with deep insights into suspicious files and URLs that may evade traditional detection methods. SMAP offers multiple layers of analysis capabilities, allowing for comprehensive examination of potential threats in a fast and efficient manner. The platform utilizes isolated virtual environments for various phases of analysis, ensuring thorough and safe evaluation of malware behavior. SMAP's features include advanced sandboxing technology, real-time behavioral analysis, and seamless integration with existing security infrastructure such as SIEM, SOAR, and EDR/XDR platforms, the company said in a release.

In addition to this, the company also announced the launch of Seqrite Threat Intel, a real-time Cyber Defense Hub powered by Seqrite Labs, India's largest malware analysis lab. This platform is set to offer comprehensive threat intelligence from diverse sources, including open-source intelligence (OSINT) and Computer Emergency Response Teams (CERTs). Leveraging Seqrite's vast network of 8.44 million endpoints, Threat Intel will provide real-time insights and industry-specific contextualization of threats. The platform is designed to enhance situational awareness, enabling organizations to proactively detect and mitigate potential security incidents.

Vishal Salvi, Chief Executive Officer of Quick Heal Technologies, commented, "The unveiling of the 'India Cyber Threat Report 2025' alongside Seqrite Malware Analysis Platform, and Seqrite Threat Intel solution represent our comprehensive approach to addressing the evolving cybersecurity challenges faced by Indian businesses. These solutions are not just about responding to threats, but anticipating them. Our Threat Report provides critical insights and actionable recommendations, SMAP empowers security professionals with advanced analysis capabilities, and Seqrite Threat Intel will offer real-time defense mechanisms. I sincerely thank DSCI and our dedicated experts at the Labs for their relentless commitment to advancing excellence in cybersecurity and their efforts to reshape the ecosystem. These efforts ensure that our clients are always one step ahead in this digital arms race, fortifying India's cybersecurity landscape against current and future threats."

Vinayak Godse, Chief Executive Officer, Data Security Council of India, added, "The India Cyber Threat Report 2025 is an annual effort to bring out the big picture of India's cyber threat landscape, providing insights at state, city, infrastructure and industry segment levels. The increase in the demand of behavior-based detections of malware represents an important evolution in both attack and defense strategies. This tells us that attackers are creating more sophisticated ransomware that can evade traditional signature-based detection methods. I hope, the report serves as a strategic compass for organizations and leaders to navigate the threat landscape. We are glad to work with the Quick Heal team for collaborating to bring out the threat landscape in a comprehensive and nuanced manner."

These launches come at a critical time as the cybersecurity landscape continues to evolve with emerging threats such as AI-driven attacks, cloud vulnerabilities, and sophisticated ransomware campaigns targeting critical infrastructure. Seqrite's comprehensive approach combines threat intelligence, advanced malware analysis, and proactive defense mechanisms to address the unique cybersecurity challenges faced by Indian businesses and government entities. By providing these solutions and insights, Seqrite is positioning itself as a leader in India's enterprise cybersecurity space, offering solutions that not only protect against current threats but also anticipate and prepare for future challenges in the digital realm, it added.

Key Highlights:

India Cyber Threat Report 2025:

- 369.01 million malware detections across an 8.44 million-strong installation base in India.
- Signature-based detection methods still dominate at 85.44%, while behavior-based detection accounts for 14.56%.

Breakdown of malware subcategories:

- Trojans (43.38%), Infectors (34.23%), Worms (8.43%), and others.
- Telangana, Tamil Nadu, and Delhi are the top three regions affected by malware.
- Healthcare, Hospitality, and BFSI as the most targeted sectors.

Seqrite Malware Analysis Platform (SMAP):

- Advanced static and dynamic analysis capabilities for suspicious files and URLs.
- Utilizes isolated virtual environments for safe malware analysis, reducing the risk of infection.
- Seamless integration with existing security infrastructure for enhanced threat response.

Seqrite Threat Intel:

- The upcoming real-time Cyber Defense Hub powered by Seqrite Labs.
- Comprehensive threat intelligence from diverse sources, including OSINT and CERTs.
- Leverages insights from Seqrite's extensive network of 8.44 million endpoints.
- Industry-specific contextualization of threats for proactive defense and regulatory compliance.