Quick Heal

Quick Heal Technologies Ltd.
Regd. Office: Solitaire Business Hub, Office No. 7010 C & D,
7th Floor, Viman Nagar, Pune 411014. India.

Ref. No.: QHTL/Sec/SE/2024-25/50

4 December 2024

To,
The Manager,
Corporate Services,
BSE Limited,
14th Floor, P J Towers, Dalal Street,
Mumbai – 400 001
Ref: Security ID: QUICKHEAL
Security Code: 539678

To,
The Manager,
Corporate Services,
National Stock Exchange of India Limited,
Exchange Plaza, Bandra Kurla Complex,
Bandra (E), Mumbai – 400 051
Symbol: QUICKHEAL
Series: EQ

Sub: Intimation pursuant to Regulation 30 of the SEBI (LODR) Regulations, 2015 regarding New Product Launch and issue of India Cyber Threat Report 2025.

Dear Sir/Madam,

Pursuant to the provisions of SEBI (LODR) Regulations, 2015 this is to inform that the company is delighted to announce the launch of its new product on 4 December, 2024 and issue of India Cyber Threat Report 2025.

This details of the said products is provided in table below and a press release of the same is enclosed to this intimation.

Name of the Product	Seqrite Malware Analysis Platform (SMAP) and Threat Intel Solution
Date of Launch	4 December 2024
Category of the Product	Enterprise Security Software / Malware Analysis Platform and Threat Intel Solution
Whether caters to Domestic and International market	First Phase to be introduced in Domestic Market and subsequently in other geographies.

This is for your information and records.

Sincerely,
For Quick Heal Technologies Limited

Vikram Bharat Dhanani
Digitally signed by Vikram Bharat Dhanani
Date: 2024.12.04 17:12:33 +05'30'

Vikram Dhanani
Compliance Officer

SEQRITE Quick Heal DSCI PROMOTING DATA PROTECTION

Strengthening India's Cyber Defenses: Seqrite Unveils the India Cyber Threat Report 2025, Launches Malware Analysis Platform and Threat Intel Solution

- *The 'India Cyber Threat Report 2025', developed in association with DSCI, provides comprehensive insights into the country’s evolving threat landscape*
- *The study highlights 369.01 million malware detections across an installation base of 8.44 million endpoints across India*
- *Seqrite’s latest offering, the Seqrite Malware Analysis Platform, is a cutting-edge tool created to empower cybersecurity professionals to effectively analyze & identify malwares*
- *The company’s solution, Seqrite Threat Intel, is a real-time Cyber Defense Hub designed to offer comprehensive threat intelligence from diverse sources*

New Delhi, 4th December 2024: Seqrite, the enterprise arm of global cybersecurity solutions provider, Quick Heal Technologies Limited, has unveiled groundbreaking cybersecurity initiatives at the 19th nasscom-DSCI Annual Information Security Summit (AISS) 2025, reinforcing its commitment to fortifying India's digital infrastructure against evolving cyber threats.

The centerpiece of Seqrite's announcements is 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 & 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.

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 Limited**, 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."*

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.

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.

To read the full India Cyber Threat Report 2025, Click here

About Seqrite

Seqrite is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, Seqrite delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. Seqrite is the Enterprise arm of the global cybersecurity brand, Quick Heal Technologies Limited, the only listed cybersecurity products and solutions company in India.

We are the first and only Indian company to have solidified India's position on the global map by collaborating with the Govt. of the USA on its NIST NCCoE's Data Classification project. We are differentiated by our easy-to-deploy, seamless-to-integrate comprehensive solutions providing the highest level of protection against emerging and sophisticated threats powered by state-of-the-art threat intelligence and playbooks backed by world-class service provided by best-in-class security experts at India's largest malware analysis lab – Seqrite Labs. We are the only Indian full-stack company aligned with CSMA architecture recommendations, offering award-winning Endpoint Protection, Enterprise Mobility Management, Zero Trust Network Access, and many more. Seqrite Data Privacy management solution enables organizations to stay fully compliant with the DPDP Act and global regulations.

Today, 30,000+ enterprises in more than 70 countries trust Seqrite with their cybersecurity needs. For more information, please visit: https://www.seqrite.com/

About Quick Heal Technologies Limited

Quick Heal Technologies Ltd. is a global cybersecurity solutions provider. Each Quick Heal product is designed to simplify IT security management across the length and depth of devices and on multiple platforms. They are customized to suit consumers, small businesses, government establishments, and corporate houses. Over a span of nearly 3 decades, the company's R&D has focused on computer and network security solutions.

The current portfolio of cloud-based security and advanced machine learning-enabled solutions stops threats, attacks, and malicious traffic before it strikes. This considerably reduces the system resource usage. The security solutions are indigenously developed in India. Quick Heal Antivirus Solutions, Quick Heal Scan Engine, and the entire range of Quick Heal products are proprietary items of Quick Heal Technologies Ltd. Recently, unveiled Quick Heal pioneers India's first fraud prevention solution, AntiFraud.AI available for Android, iOS and Windows.

For more information, please visit: https://www.quickheal.co.in/

About Data Security Council of India (DSCI)

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.