Seqrite Reveals Key Insights into the Rising Instances of Income Tax-themed Scams

Seqrite, the enterprise security arm of Quick Heal Technologies Limited, a global provider of cybersecurity solutions, has uncovered a devastating Income Tax-themed phishing campaign targeting unsuspecting users. Attackers are leveraging the tax season's urgency to breach corporate networks and drain sensitive data. The threat was uncovered by a team of researchers at Seqrite Labs, India's largest malware analysis facility, who revealed that attackers are exploiting government authority to distribute Remote Access Trojans to Indian businesses. Scammers imitate official Income Tax Department notices to trick employees into downloading malware that grants attackers complete remote control over compromised systems.

The campaign begins with a deceptive spear-phishing email appearing to come from the Income Tax Department, complete with the Government of India emblem, official letterheads and fabricated compliance deadlines. The sender address, however, originates from a public Outlook account, which is a telltale sign that no authentic government agency uses free email services for official communications. The email contains no visible text, only an image that looks identical to a real tax notice, a tactic designed to slip past email filters that scan for dangerous words. Attached is a PDF titled "Review Annexure.pdf" that claims the recipient has failed to comply with a tax review issued on October 3, 2025, creating artificial pressure to act immediately.

Opening the PDF leads victims to a seemingly official "Compliance Portal", which immediately triggers a forced download of a ZIP file named "Review Annexure.zip". The site includes a message claiming that antivirus programs may conflict with the tax portal and suggests disabling security software. This is another sign for users to look out for, since no government agency ever asks users to turn off protection. Inside the downloaded ZIP lies a 150MB executable file bearing a digitally signed certificate from a Chinese company, "Hengshui Shenwei Technology Co., Ltd.", a forgery tactic designed to appear legitimate. Once executed, this two-stage NSIS installer silently unpacks multiple components into hidden system directories without showing any visible installation interface. The first stage erases itself, leaving almost no traces, while the second stage deploys a full remote access and Windows Real-time Protection Service.

Once embedded, the malware begins collecting sensitive system information, including but not limited to operating system versions, installed applications, running services, hardware details and user activity logs. It stores this stolen information in an encrypted, hidden folder and uploads it to multiple command-and-control servers in China, using non-standard ports to evade detection. From there, attackers can remotely task the infected computer to steal files, monitor activity, install additional malware or launch attacks into the victim's company network.

Seqrite's India Cyber Threat Report 2026, drawing from telemetry across over 8 million endpoints, reveals that the Indian malware ecosystem remains dominated by Trojans (43%), File Infectors (35%), and Potentially Unwanted Applications (6%). This is a clear reflection of attackers' continued success through social engineering, cracked software, and legacy vulnerabilities. According to researchers at Seqrite Labs, such campaigns exemplify a complex and sophisticated execution of psychological manipulation and technical stealth that can damage any organization, regardless of size or sector. A single careless click on a malicious link or downloaded file can turn an entire corporate network into an attacker's playground, enabling espionage, sabotage or data theft on a massive scale.

Seqrite's India Cyber Threat Report 2026 further highlights a worrying gap in data privacy governance across organisations, where many still lack mature controls around data classification, leakage prevention and secure data handling. Modern phishing and remote access campaigns increasingly aim not just to infect systems, but to exploit identity access and extract sensitive data that often goes undetected. As enterprises move toward cloud and hybrid environments, endpoint security alone is no longer sufficient, making continuous monitoring of identity misuse and data access critical to preventing silent breaches. Therefore, it is recommended that organizations must treat every unsolicited email with extreme caution.

Users must verify any compliance request by calling the Income Tax Department directly using phone numbers from the official incometaxindia.gov.in website, and never through numbers provided in suspicious emails. Also, avoid downloading files or clicking on links from unexpected messages, and always type official URLs manually into browsers rather than trusting email hyperlinks. Enable multi-factor authentication on all critical business accounts and implement strict email gateway controls that scan for embedded images, fake compliance portals and obfuscated code.

Adavanced cybersecurity solutions from Quick Heal Technologies Limited, such as Quick Heal Total Security version26 with AntiFraud.AI for retail users and SMEs, and Seqrite's range of enterprise-grade security products, stand as a critical shield of protection against such threats. By detecting and blocking phishing payloads, malicious certificates and remote access trojans in real time before they execute, these solutions safeguard users from credential theft and supply-chain compromise, turning would-be victims into well-protected defenders.