THE HINDU businessline.

Seqrite uncovers Income Tax-themed phishing attack targeting Indian businesses

The malware collects system information, stores it in encrypted folders, and transmits it to command-and-control servers in China using non-standard ports.

ttackers are impersonating official notices to trick employees into downloading Remote Access Trojans (RATs). Victims are redirected to a fake compliance portal that forces a malware download, enabling attackers to gain full remote access. | Photo Credit:

Seqrite, the enterprise security arm of Quick Heal Technologies Limited, has uncovered a large-scale Income Tax-themed phishing campaign targeting Indian businesses. The threat, identified by researchers at Seqrite Labs, India’s largest malware analysis facility, exploits the urgency of tax season to distribute Remote Access Trojans (RATs) and breach corporate networks.

According to Seqrite, attackers impersonate official Income Tax Department notices to trick employees into downloading malware that grants complete remote access to compromised systems. The campaign begins with a spear-phishing email bearing the Government of India emblem, official letterheads and fabricated compliance deadlines. However, the sender address originates from a public Outlook account. The email contains only an image resembling a tax notice to evade text-based email filters and includes a PDF attachment titled “Review Annexure.pdf.”

Opening the PDF redirects victims to a fake “Compliance Portal” that forces the download of a ZIP file named “Review Annexure.zip.” The site also advises disabling antivirus software. Inside the ZIP is a 150MB executable file digitally signed under the name “Hengshui Shenwei Technology Co., Ltd.” Once executed, the installer silently deploys malware into hidden system directories.

The malware collects system information, stores it in encrypted folders, and transmits it to command-and-control servers in China using non-standard ports. Attackers can then steal files, monitor activity or launch further attacks.

Seqrite’s India Cyber Threat Report 2026, based on telemetry from over 8 million endpoints, shows Trojans account for 43% of threats, followed by File Infectors (35%) and Potentially Unwanted Applications (6%).