ET CISO.in
From The Economic Times

Operation XENOFISCAL reveals sophisticated cyber espionage

A cyber espionage campaign named Operation XENOFISCAL has been uncovered. This operation targets Indian finance and revenue systems. Advanced threat group SideCopy is behind the attack. They use XenoRAT malware. The campaign employs sophisticated phishing and fileless techniques. This highlights vulnerabilities in government systems. It underscores the need for enhanced cybersecurity measures.

Segrite has disclosed details of Operation XENOFISCAL, a targeted cyber espionage campaign attributed with medium-to-high confidence to SideCopy, an advanced persistent threat group operating under the broader Transparent Tribe/APT36 umbrella.

Researchers found that the operation deploys a persistent variant of XenoRAT 1.8.7 across finance ministry and provincial revenue systems, using carefully crafted local-language spear-phishing lures and a multi.

Researchers found that the operation deploys a persistent variant of XenoRAT 1.8.7 across finance ministry and provincial revenue systems,

using carefully crafted local-language spear-phishing lures and a multi-stage, largely fileless infection chain that abuses legitimate Windows binaries to bypass traditional defenses.

The campaign begins with a spear-phishing email carrying a ZIP archive that appears to be a routine internal document. Inside is a malicious Windows shortcut file with a local-language filename translating to "List of Employees Who Were Introduced to the Intellectual and Psychological Warfare Seminar." The theme appears tailored to government staff workflows:

Once the shortcut is executed, it abuses the legitimate Windows utility mshta. exe as a living-off-the-land binary to fetch a remote HTML Application from a compromised education domain. The attack then executes heavily obfuscated JavaScript directly in memory, reducing the likelihood of detection.

The campaign proceeds through several in-memory stages. A heavily obfuscated Script payload reconstructs malicious components using hex-encoded arrays, custom Base64 routines and NET deserialization, ultimately loading a .NET DLL-based first-stage loader.

While the victim is shown a realistic decoy document containing a detailed finance ministry staff directory, the loader creates a new directory under the Public user profile, establishes registry-based persistence under a typosquatted "Edgre" entry designed to mimic Microsoft Edge, and prepares the system for the final payload.

In the final stage, the infection deploys XenoRAT 1.8.7, an open-source remote access trojan configured to communicate over TCP with attacker-controlled infrastructure hosted on European bulletproof servers, including the command-and-control IP 185.235.137.106.

Once active, XenoRAT provides the operator with post-exploitation capabilities, including remote command execution, dynamic DIL loading, file exfiltration, scheduled task creation, antivirus reconnaissance, SOCKS5 proxy tunneling, keystroke logging, screenshot capture, clipboard monitoring, webcam and microphone surveillance, and the ability to remove persistence traces or uninstall itself.

By relying on staged, in-memory execution and trusted components such as mshta.exe, the operation leaves a limited forensic footprint on disk while maintaining access to fiscal and personnel data inside government

systems.

Researchers noted that Operation XENOFISCAL reflects a broader regional pattern in which threat groups use customized open-source remote access trojans, local-language lures and overseas infrastructure to complicate attribution. The use of a compromised education domain and a genuine finance-related staff directory as a decoy suggests prior reconnaissance and data harvesting.

For governments and critical institutions across the region, the implications go beyond endpoint compromise. Finance ministries, tax authorities and provincial revenue offices hold sensitive information such as budgets, revenue flows, payroll data, contracts, and records on officials and vendors. Compromise of these systems can support espionage, coercion, fraud or economic disruption.

In India, where fiscal, identity and benefits data are central to governance, the Digital Personal Data Protection Act, 2023 increases accountability for organisations handling personal data. Such intrusions highlight the need for stronger visibility, data governance, identity controls, and incident response capabilities across public-sector afid critical infrastructure environments.

The campaign shows how attackers are targeting poorly inventoried, overexposed and weakly governed information assets. It also reinforces the need for stronger endpoint monitoring, email security, threat intelligence, data protection controls and faster investigation of suspicious activity across government and enterprise environments.