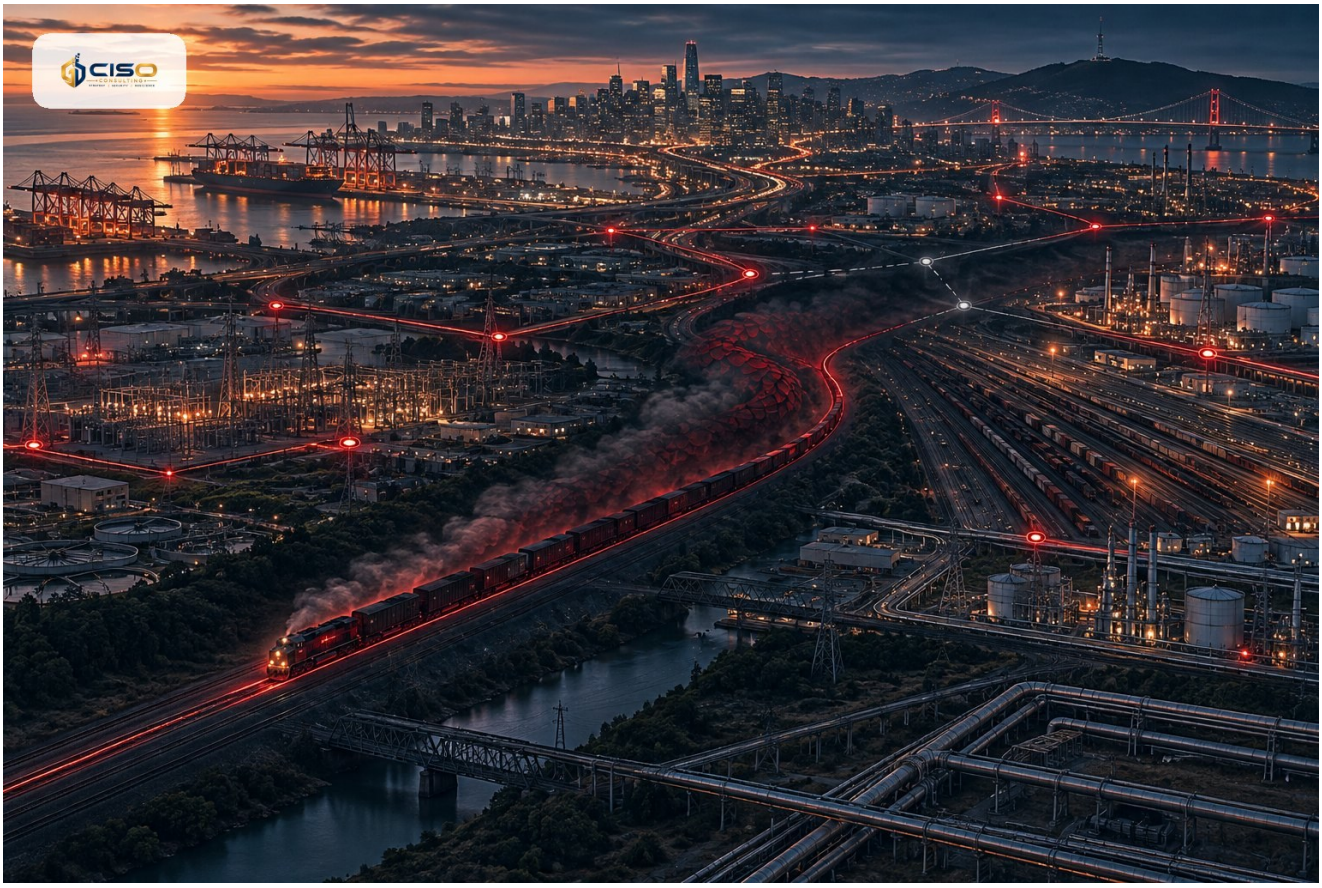
Volt Typhoon linked to disrupted 'Silent Train' covert access network



Lumen's Black Lotus Labs attributes a now-disrupted covert access network, Silent Train, to the China-nexus group Volt Typhoon. It was used for zero-day exploitation and strategic access.

- Volt Typhoon is described as a China-nexus cyber espionage group.
- The covert network, named Silent Train, has been disrupted.
- Lumen Technologies Black Lotus Labs says it was first identified in late 2023.
- It relies on rotating chains of compromised SOHO, IoT and enterprise infrastructure.
- The network was used for zero-day exploitation and strategic access.

Lumen Technologies' Black Lotus Labs has attributed a covert access network, dubbed Silent Train, to Volt

Typhoon, a China-nexus cyber espionage group. The network has now been disrupted. According to the report, it was used for zero-day exploitation and for strategic access.

What the report describes

Black Lotus Labs says Silent Train was first identified in late 2023. It works through rotating chains of compromised small-office/home-office (SOHO) devices, IoT devices and enterprise infrastructure. Routing activity through such chains makes the origin of malicious traffic harder to see.

The source excerpt available to us does not give further detail, such as affected products, victims or technical indicators, so we do not draw conclusions on those points.

Why it matters for regulated institutions

The reported use of ordinary edge and IoT devices as relay points is a reminder that unmanaged or poorly maintained equipment can become part of someone else's attack infrastructure. Disruption of one network does not remove that wider risk.

Institutions should treat this as a prompt to review their own exposure rather than as a sign of a specific threat to them. Review the full Black Lotus Labs report when it is available for indicators and mitigations.

What to do now

1. Inventory internet-facing SOHO, IoT and edge devices, including those at branches and remote sites.
2. Patch or replace end-of-life edge devices and remove unneeded external exposure.
3. Review logs for unusual inbound or outbound connections from edge and IoT devices.
4. Read the full Black Lotus Labs report and apply any published indicators to monitoring.
5. Confirm zero-day response procedures, including emergency mitigation and escalation paths.