Webworm suspected of using a modified SoftEther VPN Bridge for covert access



A China-aligned actor, Webworm, is suspected of running a customised SoftEther VPN Bridge, disguised as network-monitoring software, to keep covert remote access to compromised networks and avoid detection.

- Webworm is described as a China-aligned threat actor.
- It is suspected of using a custom build of the open-source SoftEther VPN Bridge.
- The changes reportedly aim to remove fingerprints that security tools recognise.
- The tool is disguised as network-monitoring software.
- The purpose is covert remote access to compromised networks.

What was reported

Webworm, a threat actor described as China-aligned, is suspected of using a customised version of the open-source **SoftEther VPN Bridge**. According to the report, the modified variant removes the recognisable fingerprints that detection tools usually rely on and implements several techniques to hide itself from security tooling.

The tool is also reportedly presented as network-monitoring software. The aim is to establish covert remote access to networks the actor has already compromised.

Why it matters

SoftEther is a legitimate, widely available VPN tool, so signature-based detection of the standard build may not catch a modified copy. A process or service that looks like a monitoring product can pass casual review by administrators. Attribution and the full technical detail remain with the original reporting, and the activity is described as suspected.

Practical reading for security teams

The useful lesson is to treat unexpected VPN or tunnelling capability on servers as a finding in its own right, whatever the software is called. Behaviour-based checks, such as unusual outbound tunnels, unapproved services and monitoring tools absent from the asset inventory, are more reliable than name or signature matching for this kind of tool.

What to do now

1. Search servers and endpoints for SoftEther components, including renamed binaries and services presented as monitoring tools.
2. Reconcile every installed monitoring or remote-access tool against the approved asset and software inventory.
3. Add detections for unexpected VPN tunnels and unusual long-lived outbound connections from servers.
4. Restrict outbound traffic from servers to approved destinations and review egress logs.
5. Apply application allow-listing on critical servers so unapproved network tools cannot run.
6. If a match is found, escalate through the incident process and follow NCA incident reporting obligations.