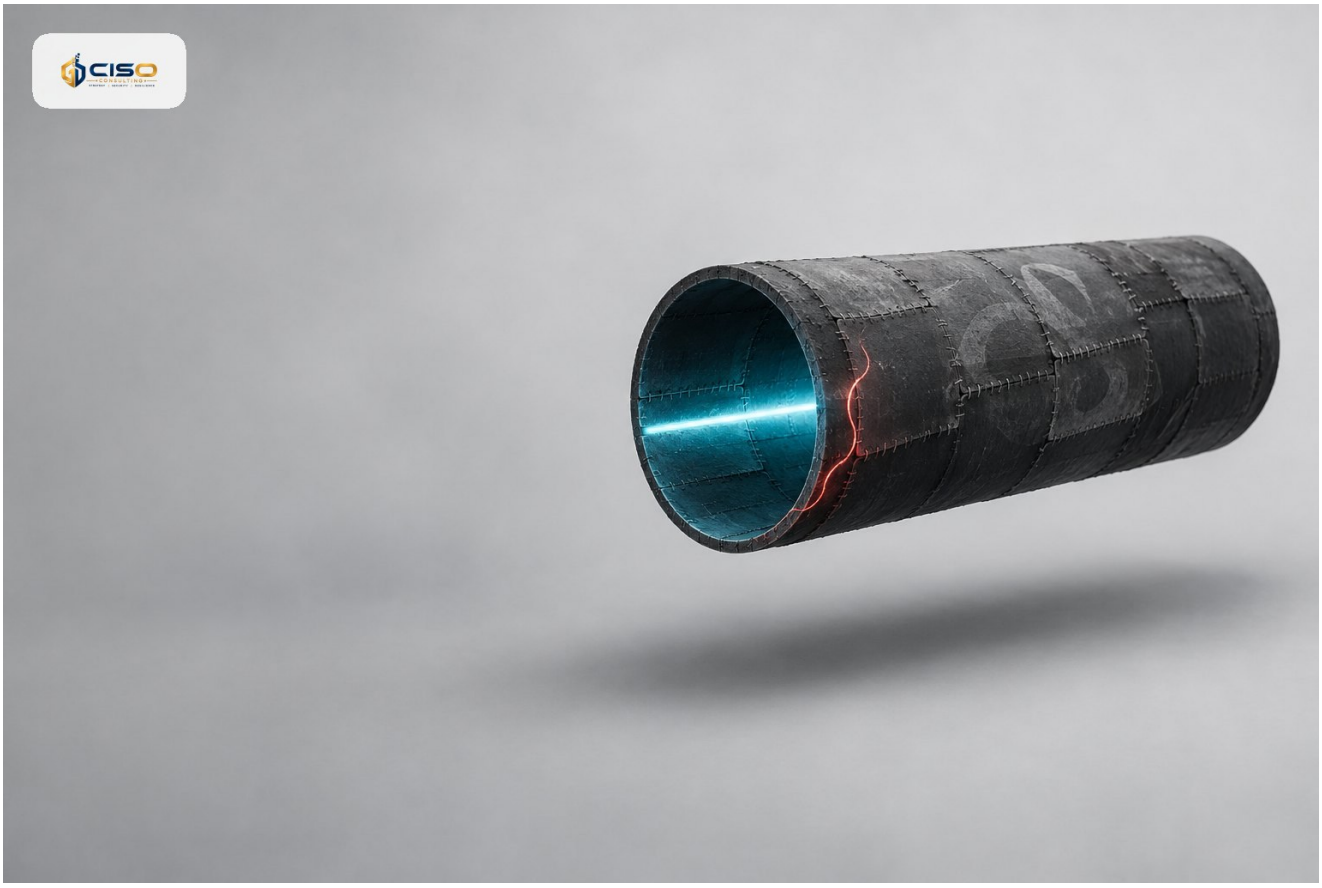
Webworm APT Uses Customized SoftEther VPN to Evade Defenders



A China-aligned espionage group known as Webworm rebuilt the open source SoftEther VPN from source code, removing artifacts that usually reveal it to defenders. Teams should review how they detect unauthorized VPN software.

- Webworm is described as a China-aligned espionage group.
- The group rebuilt the open source SoftEther VPN software from source.
- The custom build strips out artifacts that would normally expose it to defenders.
- Detection that depends on known default features of the software may therefore miss it.

What was reported

Dark Reading reports that Webworm, an espionage group aligned with China, has been using a customized version of SoftEther VPN. Rather than deploying the standard release, the group compiled the open source software itself from source code.

Building the software this way allowed the group to remove the artifacts that would normally give it away. Those are the traits defenders typically rely on to recognize the tool on a network.

Why it matters

SoftEther is legitimate, freely available software. When an attacker recompiles it and strips its identifying traits, detection rules built around the stock version may no longer match. The tool can then blend into ordinary network activity and give the actor a quieter channel into an environment.

The source summary does not describe victims, regions, or technical indicators, so institutions should not assume they are or are not affected based on this report alone.

Practical view

The useful lesson is not specific to one tool. Defenses that rely only on known signatures for remote-access software are weaker against modified builds. Behavioral monitoring, an accurate inventory of approved remote-access tools, and egress controls give broader coverage. Security teams in regulated institutions can use this report as a prompt to test whether an unapproved VPN service would be noticed today.

What to do now

1. Maintain an inventory of approved remote-access and VPN tools and flag anything outside it.
2. Add behavioral detections for unexpected VPN-like tunnels and unusual outbound connections, not only signature-based rules.
3. Review egress filtering to restrict which hosts can open outbound tunnels.
4. Hunt for SoftEther-related activity, including recompiled or renamed builds, on servers and endpoints.
5. Test whether your monitoring would detect an unapproved VPN service and close any gaps found.