Webworm APT

group · Webworm first reported 19 Nov 2026 3 sources v2 · updated 23 Nov 2026, 18:52 UTC

also reported as a China-aligned nation-state group · China-aligned APT

ACTIVE

> *"we share our analysis of what we believe to be a so-far unknown custom SoftEther-based tool, which implements various tricks to hide itself from security tools, and which we attribute to Webworm with moderate confidence."* [1]

BOTTOM LINE

Webworm is using a custom SoftEther VPN Bridge (NtMonitor) to hide persistent access into government networks; it's stealthy but targeted. Investigate any SoftEther-like services, renamed binaries, or unusual outbound connections now. Detection requires correlating executable metadata, service registrations, and anomalous POSTs to /update/picture.cgi.[1,2,3]

FOR THE BOARD

A China-aligned group is using a rebuilt SoftEther VPN to stealthily tunnel into government networks; investigate any SoftEther-like services and unusual outbound tunnels immediately.

ARE YOU EXPOSED?

TARGETS compromised government networks using modified SoftEther VPN Bridge (NtMonitor).[1,2]

look for SoftEther-like services, netcapa.exe/NtMonitor labels, setting.conf, and POSTs to /update/picture.cgi.

WHAT TO DO

1. **Search endpoints for SoftEther binaries and netcapa.exe filenames.**[1,2]
   the sample presents as netcapa.exe and is a rebuilt SoftEther bridge used to maintain covert access.
2. **Hunt for services registering SEVPNBRIDGE or NtMonitor strings and renamed registry keys.**[1,2]
   the modified build still uses SEVPNBRIDGE entry point and embeds NtMonitor labels in service and registry strings.
3. **Inspect network logs for POST requests to /update/picture.cgi with image/jpeg but PNG signature.**[2]
   the modified bridge uses that path and a PNG watermark mismatch to hide protocol handshakes.
4. **Extract and decrypt setting.conf files starting with ASCII RCEN where found.**[2,3]
   the tool stores encrypted configs in setting.conf with RCEN marker and embedded RC4-like key for recovery.

Timeline

2026-11-19 PUBLISHED	DISCLOSURE	analysis published [1] *“we share our analysis of what we believe to be a so-far unknown custom SoftEther-based tool, which implements various tricks to hide itself from security tools, and which we attribute to Webworm with moderate confidence.”*
2026-11-21 PUBLISHED	DISCLOSURE	secondary reporting [2] *“The November 19 analysis describes a Windows executable that preserves SoftEther’s network bridging capabilities while changing the artifacts defenders use to identify unauthorized deployments.”*
2026-11-23 PUBLISHED	DISCLOSURE	additional reporting [3] *“The China-aligned threat actor known as Webworm is suspected to be using a custom version of the open-source SoftEther VPN Bridge tool in an attempt to remove recognizable detection fingerprints, while disguising it as network-monitoring software to establish covert remote access to compromised networks.”*

What they did

analysis of a public sample of a modified SoftEther VPN Bridge attributed to Webworm. [1]

“To illustrate how the tool works, we will use the only public sample of this tool we are aware of, which can be found in our IoCs list (90e7…).”

reporting that the modified bridge preserves bridging capability while changing detection artifacts. [2]

“The November 19 analysis describes a Windows executable that preserves SoftEther’s network bridging capabilities while changing the artifacts defenders use to identify unauthorized deployments.”

Whom they target

government organizations (targeted historically and in reports) [3]

“Webworm is the name assigned to a China-aligned nation-state group that has targeted government entities, IT services, and electric power companies across Russia, Georgia, Mongolia, and several other Asian nations.”

compromised governmental networks where SoftEther was deployed [1]

“which has been known to deploy the open-source SoftEther VPN into the networks of compromised governmental organizations to maintain low-profile, long-term access.”

Malware and tools

custom SoftEther VPN Bridge build labeled NtMonitor (based on v4.44 build 9807). [1]

“Based on cleartext strings and constants in the binary, we identified it as a (modified) build of the SoftEther VPN Bridge executable, specifically version 4.44, build 9807.”

embedded hamcore.se2 resource and modified handshake watermark (PNG-based). [3]

“Reducing a resource archive named hamcore.se2 used by SoftEther VPN to its bare minimum, as it's required to be present at runtime, and embedding it directly into the executable, causing the binary's size to increase by about 1.5 MB.”

Attribution

attributed to Webworm with moderate confidence. [1]

“we attribute to Webworm with moderate confidence.”

described as China-aligned and previously linked to government targeting. [3]

“The China-aligned threat actor known as Webworm is suspected to be using a custom version of the open-source SoftEther VPN Bridge tool in an attempt to remove recognizable detection fingerprints, while disguising it as network-monitoring software to establish covert remote access to compromised networks.”

Disruption, advisories and law enforcement

None reported.

ATT&CK techniques

The sources do not describe the attacker's behaviour closely enough to map.

Indicators

None published in the sources.

Not known yet

- number of victims or infections
- initial compromise vector used to deploy the bridge
- whether active command-execution backdoor exists beyond SoftEther functionality
- presence of other builds besides the public sample

Sources

1 **Rapid7 blog** · 19 Nov 2026 · Spying on Governments with Zero Lines of Malware: A Custom SoftEther Bridge in Webworm’s Toolkit · `archived copy`

2 **GBHackers** · 21 Nov 2026 · China-Linked Webworm Hackers Deploy Custom SoftEther VPN to Maintain Hidden Access to Government Networks · `archived copy`

3 **The Hacker News** · 23 Nov 2026 · Webworm Suspected of Modifying SoftEther VPN to Evade Detection and Hide Remote Access · `archived copy`

ABOUT THIS REPORT

Compiled by Transilience Newsroom from 3 public sources. Every quotation is checked against the article it cites; 5 statements were left out because the source did not bear them out. The status is never stated more strongly than its quote shows. ATT&CK techniques marked “mapped by Newsroom” are our reading of the quoted behaviour, not the source's claim. Version 2, written 23 Nov 2026, 18:52 UTC (threat-report-2026-09-25b).