Liminal Panda uses SIGweaver to target 4G Mobile Diameter protocols

Original report published on: Jan 21, 2026

Executive Summary

On 21 January 2026, Crowdstrike Intelligence identified SIGweaver attributed to Liminal Panda group, with moderate confidence, with a history of targeting the telecommunications sector. SIGweaver is a Linux kernel-level driver that covertly inserts malicious messages into the legitimate traffic flows of telecom networks without new network connections.

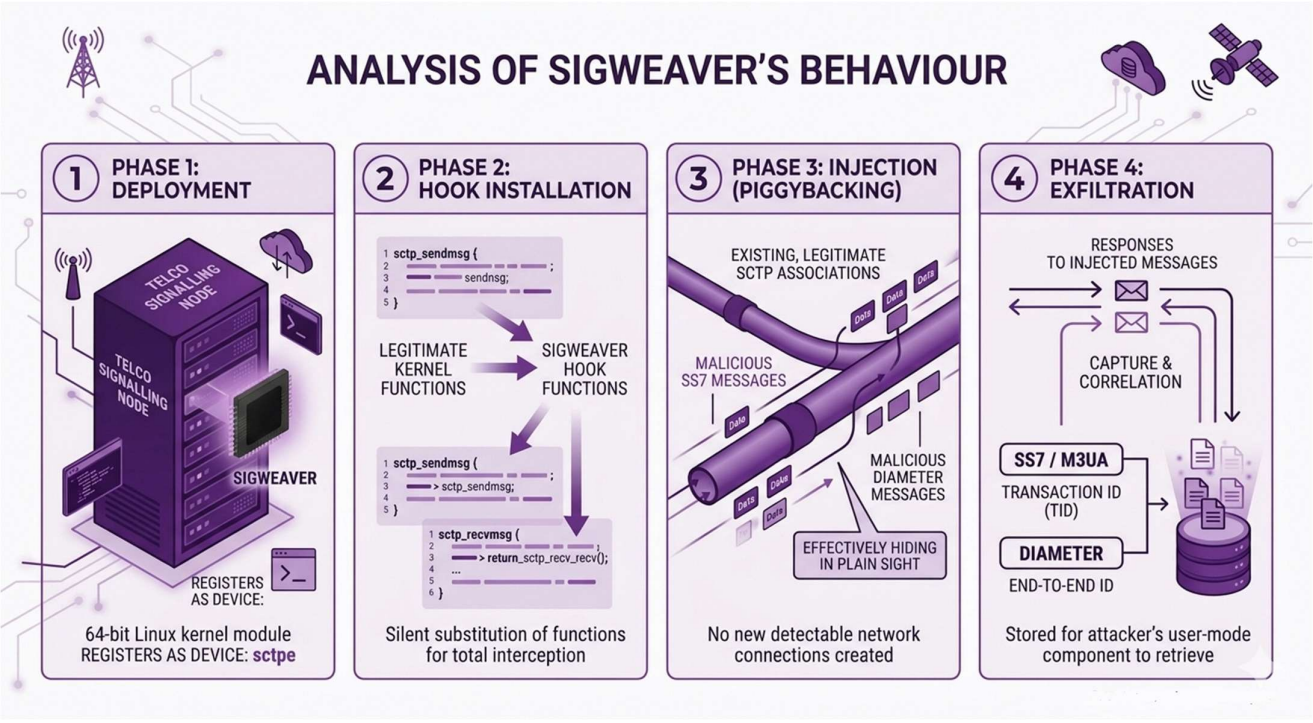
SIGweaver presents a capability upgrade as it impacts 4G LTE networks, beyond older 2G and 3G networks. If successfully deployed, SIGweaver enables adversaries the ability to harvest subscriber data, physical location, conduct denial-of-service attacks, or establish a hidden command-and-control (C2) communication within the network.

Background

About Liminal Panda

With a focus on telecommunications networks, this group previously deployed malware SIGTRANslator which is used to send signalling messages to telecom transport nodes.

About SIGweaver



Google. (2026). *Nano Banana 2* [Text-to-image model]. https://gemini.google.com

SIGweaver is a 64-bit Linux character device driver that operates at the kernel. This driver is unique, deployed in specific Linux servers, used in telecom signalling environments. SIGweaver first registers as a new character device named *sctpe*, creating the device file */dev/sctpe*. Then, it hooks into the kernel's core

SCTP send and receive functions to monitor all signalling traffic passing through the server. The attacker supplies SIGweaver with both the target peer node's address and port, as well as pre-crafted signalling messages stored in the driver's memory. SIGweaver then waits for legitimate outbound traffic to occur and appends its own malicious messages to those existing flows.

The tool supports two primary signalling protocols:

- SS7 / M3UA (used in 2G and 3G networks): Enables injection of Transaction Capabilities Application Part (TCAP) messages, which can be used to query subscriber data and location information.
- Diameter (used in 4G LTE networks): It is an authentication, authorisation and accounting protocol. Injected Diameter messages can request roaming subscriber profiles or spoof requests to cause service disruptions and enable location tracking.

The inclusion of Diameter support is a significant aspect of SIGweaver, as it marks Liminal Panda's first confirmed capability to operate natively within 4G infrastructure. In terms of targets, SIGweaver focuses on core network applications including the NMS, HSS, VLR, and SGSN.^

Operating Modes

SIGweaver has two distinct behavioural modes. First, a standard injection mode where the driver correlates its outgoing malicious requests with incoming responses using unique message identifiers embedded in the signalling headers. This is the mode most likely used for active intelligence gathering operations - querying subscriber data or tracking individuals. Second, in covert C2 mode, if SIGweaver is installed on both the source and destination nodes of a signalling path, it can use standard telecom signalling messages as a hidden data channel, effectively tunnelling attacker communications through the telecom network's own infrastructure.

Stealth and Operational Security

SIGweaver is engineered to avoiding detection. It does not create new network connections,and instead rides on pre-existing, trusted SCTP associations. When it intercepts and copies a response, it overwrites the original data with meaningless content, so that legitimate network components see an error rather than evidence of interception. The tool includes extensive debugging and tracing capabilities, indicating that Liminal Panda is a mature, operationally disciplined threat group.

Initial Access

Although it is unknown how Liminal Panda obtained initial access, the threat actor was previously observed to exploit trusted relationships, internet-facing infrastructure, valid accounts using weak passwords, services and edge devices.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the Liminal Panda-related activities identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Monitor for unauthorised or unrecognised SCTP-related kernel modules on Linux-based signalling nodes.
- Audit device files under /dev on signalling infrastructure. SIGweaver creates a device file at /dev/sctpe upon loading.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess impact prior to deploying defensive measures.

Annex A - Indicators of Compromise [Error! Reference source not found.]

SHA256 Hash
8fbc7e7998dec1c18cbe8fbe2340038cd7768e5a946a92fc1a2712101622d2e5

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Defense Evasion	T1014	Rootkit
Command and Control	T1095	Non-Application Layer
Impact	T1565.002	Data Manipulation: Transmitted Data Manipulation

Footnotes

^NMS – Network Management: The NMS or NM is top-level operations system in a PLMN (Public Land Mobile Network) that provides end-to-end visibility and control across all network elements and domains, performing fault, configuration, accounting, performance, and security (FCAPS) management via standardised interfaces.

HSS – Home Subscriber Server: The HSS is the master user database in 4G/LTE (EPC) and IMS architectures. It stores subscriber identity and profile data, authentication and security credentials (AKA vectors), location information (which MME/SGSN is serving the user) and service subscription data.

VLR – Visitor Location Register: The VLR is a temporary local database co-located with the MSC (Mobile Switching Centre) in 2G/3G circuit-switched (CS) networks. It holds a copy of subscriber data downloaded from the HLR for currently visiting User Equipment, location area information of active subscribers, TMSI (Temporary Mobile Subscriber Identity) assignments.

SGSN – Serving GPRS Support Node: The SGSN is a core packet-switched node in 2G (GPRS/EDGE) and 3G (UMTS) networks. Its key responsibilities include mobility management for packet-switched (PS) data sessions, authentication and ciphering of PS connections, routing and forwarding of data packets to/from the GGSN (Gateway GPRS Support Node), session management (PDP Context activation/deactivation), interfacing with the HLR/VLR for subscriber data