NEWS RELEASE

Rapid7 Labs Identifies State-Sponsored Sleeper Cells Embedded in Global Telecommunications Networks

2026-03-26

Research reveals long-term espionage access inside telecommunications infrastructure with implications for government communications and critical systems

BOSTON, March 26, 2026 (GLOBE NEWSWIRE) -- **Rapid7** (NASDAQ: RPD), a global leader in AI-powered managed cybersecurity operations, released findings from a months-long research investigation from Rapid7 Labs, "**Sleeper Cells in the Telecom Backbone**," detailing a sustained espionage campaign conducted by a China-nexus threat actor, Red Menshen, with covert access inside global telecommunications infrastructure.

The research highlights a shift from opportunistic intrusion to deliberate, long-term pre-positioning inside telecommunications networks. These "sleeper cells" are designed to remain undetected while providing persistent visibility into subscriber activity, signaling systems, and sensitive communications—enabling ongoing intelligence collection across environments that support government, commercial, and critical infrastructure operations.

"If you have access to telecommunications infrastructure, you are not just inside one company, you are operating close to the communication layer of entire populations, which makes this type of access highly valuable and elevates detection to a national-level concern," said Raj Samani, chief scientist at Rapid7. "The activity we are seeing continues to evolve in ways that improve stealth and persistence, and organizations should treat detection as the start of investigation, not the end of it."

The research also identifies critical visibility gaps into persistence at the kernel and packet-filtering layers. Without insight into these areas, service masquerading and stealth activation techniques can remain undetected for extended periods. Organizations must have preemptive detection strategies that identify unusual service masquerading and stealth activation mechanisms before they can be leveraged for high-level intelligence collection.

Key findings:

- Persistent access in telecommunications infrastructure: Rapid7 Labs identified coordinated activity establishing long-term, dormant footholds within global telecommunications environments.
- Kernel-level stealth using BPFdoor: The campaign uses a Linux kernel-level backdoor that operates without opening ports or generating typical beaconing activity, limiting visibility for traditional endpoint and network monitoring tools.
- Weaponization of encrypted traffic: A newly identified variant of the malware now conceals command triggers within legitimate, encrypted HTTPS traffic. By abusing SSL termination points like load balancers and proxies, the actor can bypass modern security controls to activate dormant implants.
- Access to telecommunications signaling systems: The investigation found targeting of specialized protocols such as SCTP, enabling visibility into subscriber activity, including location tracking and identity-related data across 4G and 5G networks.
- Service masquerading within telecommunications environments: The malware mimics legitimate infrastructure and management services, including hardware monitoring and container components, to blend into routine operational activity.

“This is not traditional espionage, it is pre-positioning inside the infrastructure that nations depend on,” said Christiaan Beek, vice president of cyber intelligence at Rapid7. “We are seeing a persistent access model where attackers embed within core communications systems and maintain that access over extended periods.”

Rapid7 is working with organizations it believes may be impacted and, to support defenders in identifying potential BPFdoor activity, has released a free, **open-source scanning script**. The scanning script is designed to detect both previously documented BPFDoor variants and newer samples, and is available to assist organizations in proactively identifying potential compromises. Rapid7’s goal is to help defenders rapidly validate exposure and begin incident response investigations where necessary. In addition, Rapid7 has incorporated these findings across its detection capabilities, including retroactive threat hunting and updated intelligence available to customers through the Rapid7 **Intelligence Hub**.

On Thursday, March 26 at 12:20 p.m. PT at RSAC 2026 Conference in San Francisco, Christiaan Beek will be presenting the full scope of this research in his session, “**Sleeper Cells in the Telecom Backbone**.”

On Monday, March 30, Raj Samani and Christiaan Beek will discuss the findings and the impact on global telecommunications in this **exclusive webinar**.

About Rapid7

Rapid7, Inc. (NASDAQ: RPD) is a global leader in AI-powered managed cybersecurity operations, trusted to advance organizations' cyber resilience. Open and extensible, the Rapid7 Command Platform integrates security data, enriching it with AI, threat intelligence, and 25 years of expertise and innovation to reduce risk and disrupt attackers. As a recognized leader in preemptive managed detection and response (MDR), Rapid7 unifies exposure and detection to transform the cybersecurity operations of more than 11,500 customers worldwide. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn** or **X**.

Rapid7 Media Relations
Stacey Holleran
Sr. Manager, Global Communications
press@rapid7.com
(857) 216-7804

Rapid7 Investor Contact
Matt Wells
Vice President, Investor Relations
investors@rapid7.com
(617) 865-4277

Source: Rapid7