CYBER THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

February 13, 2025

RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers

Despite significant media coverage and US sanctions, RedMike (Salt Typhoon) continues to target telecommunications providers globally, including in the US.

Insikt group observed RedMike exploiting privilege escalation vulnerabilities CVE-2023-20198 and CVE-2023-20273 to compromise unpatched Cisco network devices running Cisco IOS XE software.

RedMike compromised devices of a US-based affiliate of a UK telecommunications company, a South African telco, and it attempted to exploit over 1,000 Cisco devices between December 2024 and January 2025.

Executive Summary

Between December 2024 and January 2025, Recorded Future's Insikt Group identified a campaign exploiting unpatched internet-facing Cisco network devices primarily associated with global telecommunications providers. Victim organizations included a United States-based affiliate of a significant United Kingdom-based telecommunications provider and a South African telecommunications provider. Insikt Group attributes this activity to the Chinese state-sponsored threat activity group tracked by Insikt Group as RedMike, which aligns with the Microsoft-named group Salt Typhoon. Using Recorded Future® Network Intelligence, Insikt Group observed RedMike target and exploit unpatched Cisco network devices vulnerable to CVE-2023-20198, a privilege escalation vulnerability found in the web user interface (UI) feature in Cisco IOS XE software, for initial access before exploiting an associated privilege escalation vulnerability, CVE-2023-20273, to gain root privileges. RedMike reconfigures the device, adding a generic routing encapsulation (GRE) tunnel for persistent access.

RedMike has attempted to exploit more than 1,000 Cisco devices globally. The group likely compiled a list of target devices based on their association with telecommunications providers' networks. Insikt Group also observed RedMike targeting devices associated with universities in Argentina, Bangladesh, Indonesia, Malaysia, Mexico, the Netherlands, Thailand, the United States (US), and Vietnam. RedMike possibly targeted these universities to access research in areas related to telecommunications, engineering, and technology, particularly at institutions like UCLA and TU Delft. In addition to this activity, in mid-December 2024, RedMike also carried out a reconnaissance of multiple IP addresses owned by a Myanmar-based telecommunications provider, Mytel.

Unpatched public-facing appliances serve as direct entry points into an organization's infrastructure. Sophisticated Chinese threat activity groups have shifted heavily toward exploiting these devices for initial access over the past five years. RedMike's exploitation of telecommunications infrastructure goes beyond technical vulnerabilities and represents a strategic intelligence threat. Persistent access to critical communications networks enables state-backed threat actors to monitor confidential conversations, manipulate data flows, and disrupt services during geopolitical conflicts. RedMike's targeting of lawful intercept programs and US political figures highlights the strategic intelligence objectives behind these operations and the national security threat they pose.

Organizations, particularly those in the telecommunications industry, must prioritize remediating exposed network devices, as unpatched systems remain a key initial access vector for Chinese state-sponsored threat activity groups. Network administrators should implement strict access controls, disable unnecessary web UI exposure, and monitor for unauthorized configuration changes. Individuals should use end-to-end encrypted communication methods for sensitive information, just as the Cybersecurity and Infrastructure Agency (CISA) and the Federal Bureau of Investigation (FBI) recommended, which is crucial to mitigate potential eavesdropping risks.

Additionally, governments and cybersecurity entities should improve threat intelligence sharing and impose stricter regulatory compliance for network security. While the US sanctions on RedMike-affiliated Sichuan Juxinhe Network Technology signal a more assertive and commendable stance against state-backed cyber espionage in critical infrastructure, robust international cooperation is crucial for effectively countering these persistent threats.

Key Findings

- Despite significant media coverage and US sanctions, RedMike continues to compromise telecommunications providers globally, including in the US.
- RedMike compromised Cisco network devices of a US-based affiliate of a United Kingdom (UK) telecommunications provider and a primary South African telecommunications provider.
- RedMike exploited privilege escalation vulnerabilities CVE-2023-20198 and CVE-2023-20273 to compromise unpatched Cisco network devices running Cisco IOS XE software.
- Using Recorded Future Network Intelligence, Insikt Group identified RedMike attempting to exploit over 1,000 Cisco network devices between December 2024 and January 2025.

Background

In late September 2024, media reporting (1, 2) stated that the Chinese state-sponsored group Salt Typhoon had compromised the networks of major US telecommunications companies, including Verizon (1), AT&T, and Lumen Technologies. The activity likely affected telecommunications organizations globally, with some outlets reporting that Salt Typhoon compromised at least 80 organizations. SaltTyphoon used its access to telecommunications providers to snoop on US lawful intercept targets and intercept the communications of significant US political figures. The effect of Salt Typhoon's intrusions has reached the highest levels of the US government: Cybersecurity experts have briefed the US Senate, CISA recently issued guidance on hardening telecommunications infrastructure, and CISA and the FBI issued a joint warning encouraging the use of encrypted end-to-end messaging applications for sensitive communications.

Insikt Group tracks Salt Typhoon-aligned activity as RedMike. Salt Typhoon is a group name given by Microsoft Threat Intelligence; at this time, Microsoft has not published publicly available technical details of the group's activity. The only public information Microsoft has shared confirms an overlap with two existing threat activity group names: GhostEmperor (Kaspersky) and FamousSparrow (ESET).

On January 17, 2025, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Sichuan-based cybersecurity company Sichuan Juxinhe Network Technology Co., Ltd. for their direct involvement with RedMike activity. OFAC stated that Sichuan Juxinhe Network Technology Co., Ltd. had direct involvement in exploiting US telecommunications and internet service provider companies. According to OFAC, China's Ministry of State Security (MSS) has maintained strong ties with multiple computer network exploitation companies, including Sichuan Juxinhe.

Technical Analysis

Cisco IOS XE Web UI Exploitation

Using Recorded Future Network Intelligence, Insikt Group identified that since early December 2024, RedMike has attempted to exploit over 1,000 internet-facing Cisco network devices worldwide, primarily those associated with telecommunications providers, using a combination of two privilege escalation vulnerabilities: CVE-2023-20198 and CVE-2023-20273. When successfully compromised, the group uses the new privileged user account to change the device's configuration and adds a GRE tunnel for persistent access and data exfiltration.

The privilege escalation vulnerability CVE-2023-20198 was found in the Cisco IOS XE software web UI feature, version sixteen and earlier, and published by Cisco in October 2023. Attackers exploit this vulnerability to gain initial access to the device and issue a `privilege 15` command to create a local user and password. Following this, the attacker uses the new local account to access the device and exploits an associated privilege escalation vulnerability, CVE-2023-20273, to gain root user privileges.

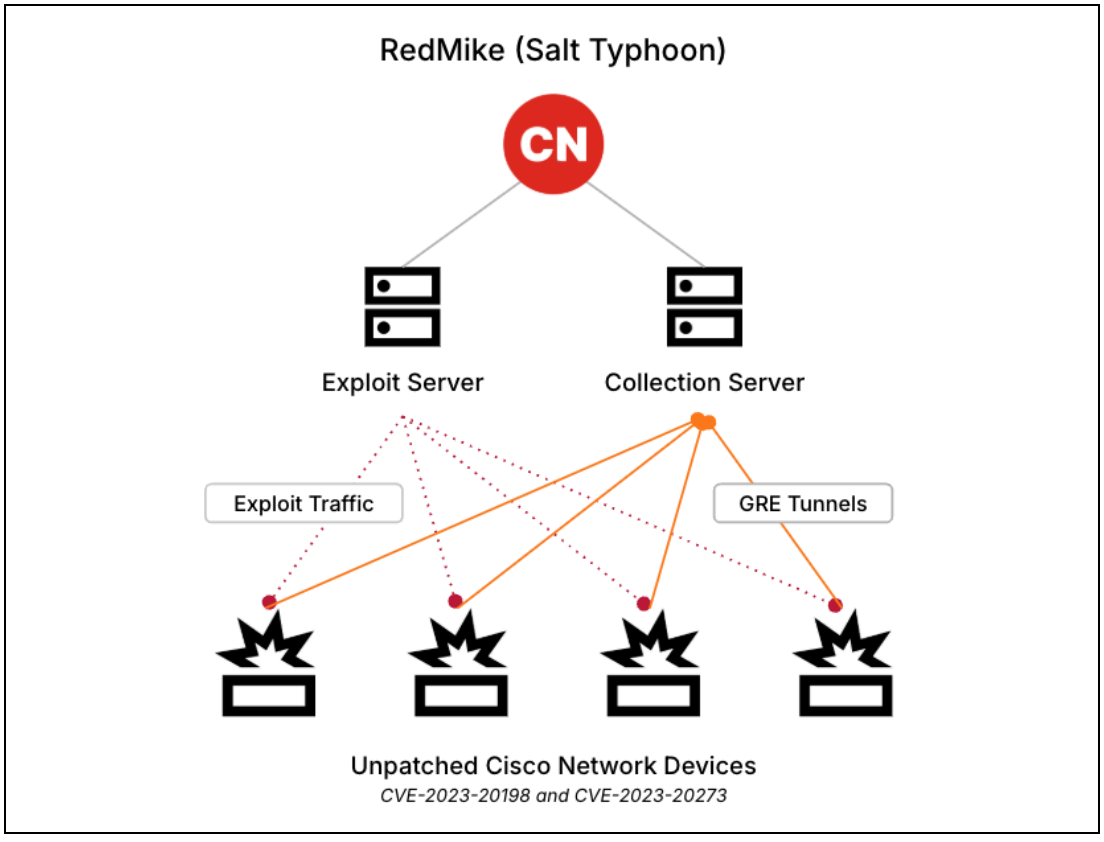


Figure 1: *RedMike Cisco network device exploitation infrastructure (Source: Recorded Future)*

More than half of the Cisco devices targeted by RedMike were in the US, South America, and India. The remaining devices spanned over 100 other countries. Although the selected devices are primarily associated with telecommunications providers, thirteen were linked to universities across Argentina, Bangladesh, Indonesia, Malaysia, Mexico, the Netherlands, Thailand, the US, and Vietnam.

Often involved in cutting-edge research, universities are prime targets for Chinese state-sponsored threat activity groups to acquire valuable research data and intellectual property. Previous examples include APT40, which has targeted universities for biomedical, robotics, and maritime research; RedGolf (APT41) for medical research; and RedBravo (APT31), which has directly targeted academics. China's cyber strategy aligns with its broader economic and military goals, making universities high-value targets for long-term intelligence-gathering and technology acquisition.

RedMike possibly targeted the following universities to access research in areas related to telecommunications, engineering, and technology, particularly at institutions like UCLA and TU Delft.

- University of California, Los Angeles (UCLA) — US
- California State University, Office of the Chancellor (CENIC) — US
- Loyola Marymount University — US
- Utah Tech University — US
- Universidad de La Punta — Argentina
- Islamic University of Technology (IUT) — Bangladesh
- Universitas Sebelas Maret — Indonesia
- Universitas Negeri Malang — Indonesia
- University of Malaya — Malaysia
- Universidad Nacional Autonoma — Mexico
- Technische Universiteit Delft — The Netherlands
- Sripatum University — Thailand
- University of Medicine and Pharmacy at Ho Chi Minh City — Vietnam

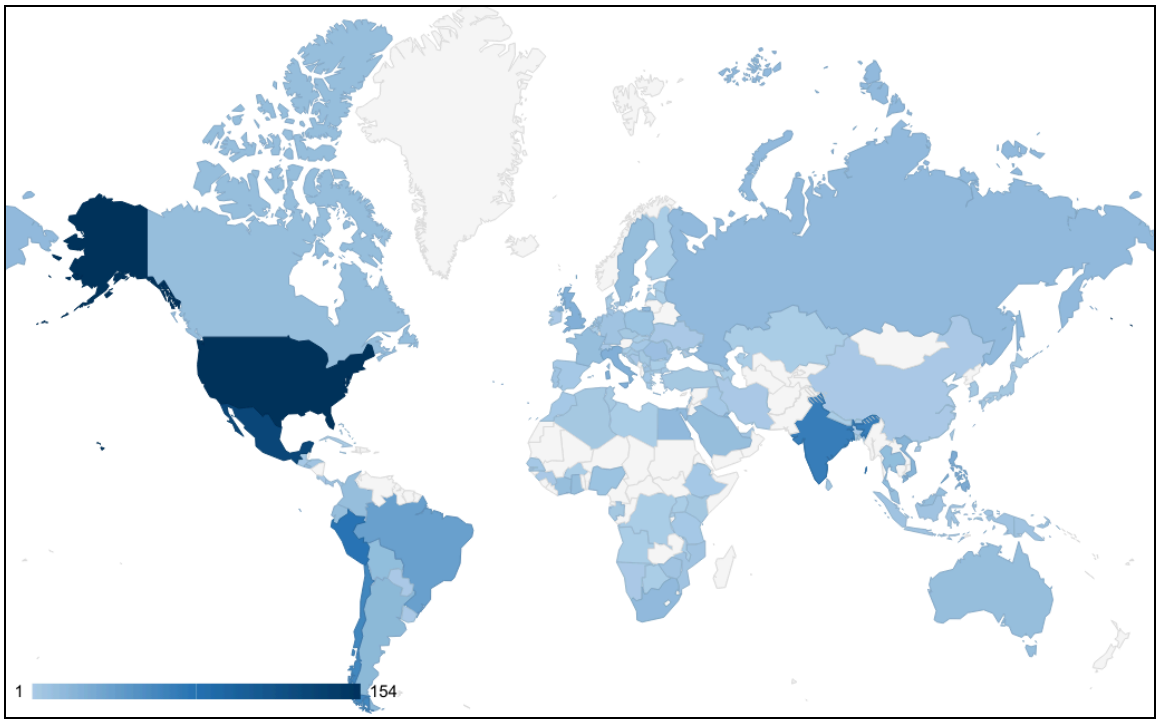


Figure 2: *Geographical spread of Cisco devices targeted by RedMike (Source: Recorded Future)*

RedMike's scanning and exploitation activity occurred on six different occasions from December 2024 to January 2025.

- 2024-12-04
- 2024-12-10
- 2024-12-17
- 2024-12-24
- 2025-01-13
- 2025-01-23

Network administrators operating a Cisco network device with IOS XE software web UI exposed to the internet can use the dates mentioned and advice in the mitigations section to identify potential RedMike exploitation activity.

Using internet scanning data, Insikt Group identified more than 12,000 Cisco network devices with their web UIs exposed to the internet. Although over 1,000 Cisco devices were targeted, Insikt Group assesses that this activity was likely focussed, given that this number only represents 8% of the exposed devices and that RedMike engaged in periodic reconnaissance activity, selecting devices linked to telecommunications providers.

Compromised Telecommunications Provider Devices

Using Recorded Future Network Intelligence, Insikt Group observed seven compromised Cisco network devices communicating with RedMike infrastructure. These include devices associated with:

- A US-based affiliate of a UK telecommunications provider

- A US internet service provider (ISP) and telecommunications company
- A South African telecommunications provider
- An Italian ISP
- A large Thailand telecommunications provider

RedMike configured GRE tunnels between the compromised Cisco devices and their infrastructure. GRE is a tunneling protocol used to encapsulate various network layer protocols inside point-to-point connections. It is a standard feature that can be configured on Cisco network devices. It is commonly used to create virtual private networks (VPNs), enable interoperability between different network types, and transport multicast or non-IP traffic over IP networks. Threat activity groups use GRE tunnels to maintain persistence by establishing covert communication channels that bypass firewalls and intrusion detection systems. These tunnels also facilitate stealthy data exfiltration by encapsulating stolen data within GRE packets, potentially bypassing network monitoring.

Reconnaissance of Myanmar Telecommunications Provider

In mid-December 2024, RedMike, from the same infrastructure that exploited the Cisco network devices, performed reconnaissance against multiple infrastructure assets operated by a Myanmar-based telecommunications provider, Mytel, likely including their corporate mail server.

Mitigations

- Prioritize applying available security patches and updates to network devices exposed to the internet.
- Avoid exposing administration interfaces or non-essential services on public-facing appliances directly to the internet, particularly for end-of-life devices.
- Monitor for network device configuration changes.
- Monitor network traffic for protocols not implemented in your network, such as GRE.
- Use the advanced query feature in Recorded Future to monitor for actively exploited technology within your stack and set alerts to notify you of any at-risk assets.

Cisco IOS XE Software Device-Specific Remediation

- Check system logs for the presence of any of the following log messages where the user could be `cisco_tac_admin`, `cisco_support`, or any configured local user that is unknown to the network administrator:
  - `%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as user on line`
  - `%SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: user] [Source: source_IP_address] at 03:42:13 UTC Wed Oct 11 2023`

Outlook

Despite significant media coverage and US sanctions, Insikt Group expects RedMike to continue targeting telecommunications providers in the US and globally due to the amount and high value of communications data that traverses these networks. This is highlighted by RedMike's previous targeting of US lawful intercept operations and the communications of significant US political figures via these intrusions.

While espionage operations are not intended to disrupt their target networks, the discovery of such a wide-ranging infiltration of US critical infrastructure has further degraded US-China relations, evidenced, for example, by the Biden administration banning China Telecom's remaining operations in the US. The US Congress has primarily focused on the security lapses at the telecommunications companies themselves, such as the presence of outdated routers and a lack of monitoring capabilities, as exemplified by the activity observed by Insikt Group.

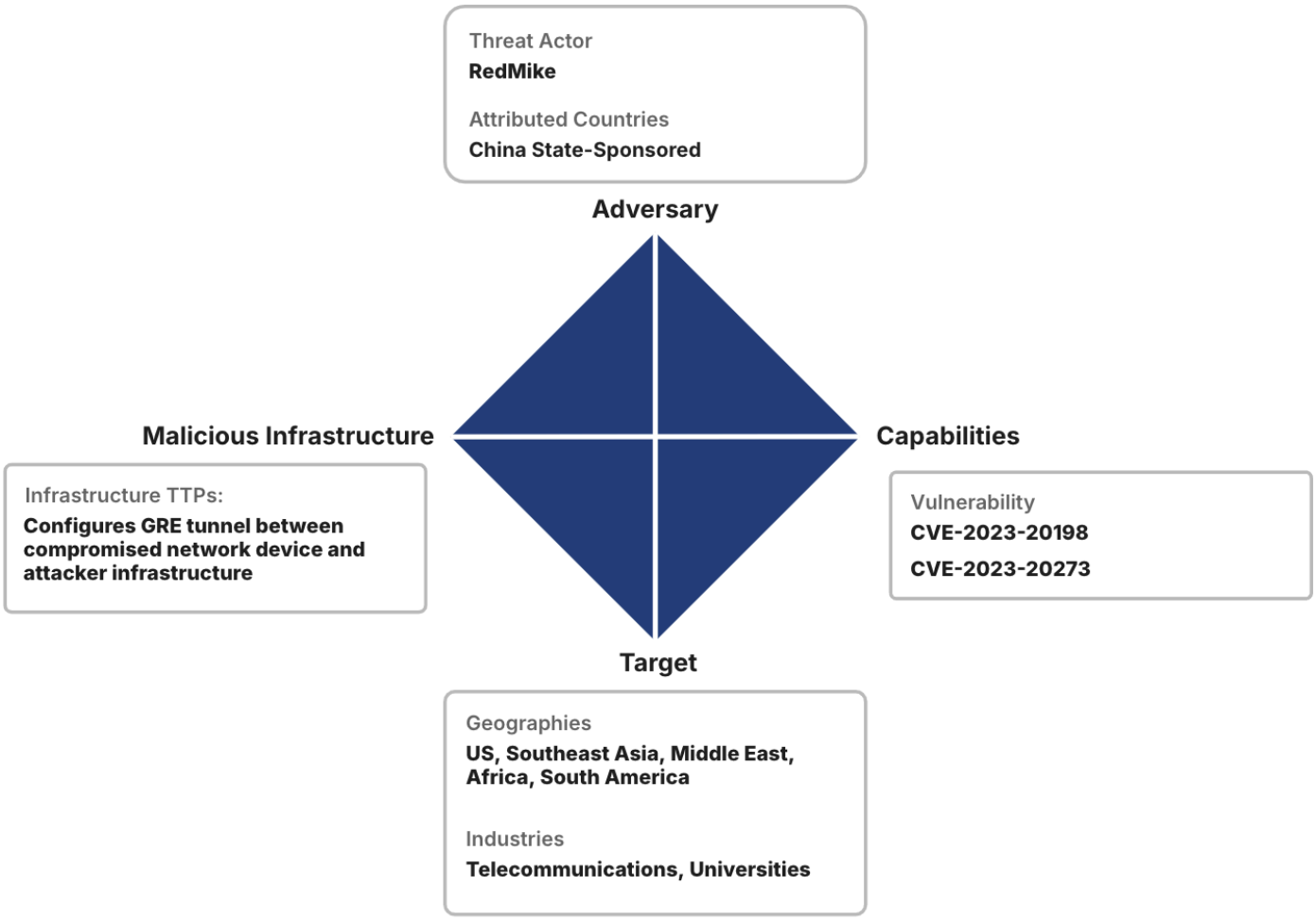
US sanctions on the entity behind RedMike's activity — Sichuan Juxinhe Network Technology Co., Ltd. — followed in early 2025, most likely further straining US-China relations. In this case, the timeline of punitive action by the US government was almost certainly accelerated by the forthcoming change in administration compared with previous actions against Chinese state-sponsored threat activity groups, which often take longer to become public (1, 2, 3). As the telecommunications industry and intelligence communities begin to grasp the scale of RedMike's intrusions and tackle the root causes, Insikt Group expects to see further technical details published.

Appendix A: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code	Observable
Initial Access: Exploit Public-Facing Application	T1190	RedMike has exploited Cisco network devices using CVE-2023-20198 for initial access.
Privilege Escalation: Exploitation for Privilege Escalation	T1068	RedMike has exploited Cisco network devices using CVE-2023-20273 to gain root-level user privileges.
Command-and-Control: Protocol Tunneling	T1572	RedMike has configured GRE tunnels between compromised Cisco network devices and attacker infrastructure.
Reconnaissance: Gather Victim Network Information	T1590	RedMike undertook a reconnaissance of Myanmar-based telecommunications provider infrastructure.
Reconnaissance: Active Scanning	T1595	RedMike has actively scanned 1,000s of Cisco network devices, attempting to exploit them with a combination of CVE-2023-20198 and CVE-2023-20273.

Appendix B: RedMike Diamond Model

RedMike
February 12, 2025



Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com