Internet-Facing Infrastructure Under Attack by China-Nexus APT Groups

C-Suite level threat review by applicable business area addressing active threats.

As 2025 reaches its half-way point, China-nexus APTs are increasingly exploiting internet-facing infrastructure. These threat actors focus on virtual private network (VPN) appliances, routers, and edge devices that often fall outside endpoint detection and response (EDR) coverage and monitoring. This strategy shows a broader shift toward targeting critical, but under secured systems in enterprise infrastructure. This newsletter will examine two China-nexus APT groups, UNC5221 and UNC3886, who highlight this trend through their targeted attacks on vulnerable edge devices and internet-facing infrastructure.

UNC5221:

UNC5221 has been active since at least 2023. The group is known for targeting critical infrastructure operators, government agencies, healthcare, defense, and finance organizations in the United States, Europe and the Middle East. This group is known for exploiting vulnerabilities in edge devices and recently exploited vulnerable Ivanti VPNs and Endpoint Manager.

UNC3886:

UNC3886 has operated since 2022 and is seen targeting vulnerabilities in systems used by the technology and telecommunication sectors in the United States and Asia. The group focuses on stealth and persistence and has recently used end of life systems to initiate their activity on networks.

UNC5221

Threat Level: Medium

Attack:

For initial access, UNC5221 often exploits zero-day vulnerabilities in internet-facing systems, particularly VPNs such as Ivanti Connect Secure (MITRE T1190). In March 2025, the group leveraged a buffer overflow vulnerability that allowed remote code execution without authentication. UNC5221 used this access to deploy TrailBlazer, which is a fileless in-memory dropper that injects a backdoor called BrushFire into the VPN's web process (MITRE T1055). This backdoor lets the attacker run commands without leaving traces on disk, making it harder for traditional security tools to detect. Once inside, the group targets the VPN's session cache database to extract sensitive information such as active session tokens, API keys, and credentials (MITRE T1003). With this access, UNC5211 can hijack live sessions without needing passwords or triggering new logins. The group exfiltrates the stolen data by disguising it as harmless web content (MITRE T1036). This allows them to quietly collect sensitive information and move deeper into the network to conduct espionage.

Remediation:

- Regularly inspect outbound HTTPS traffic from VPN appliances to identify unusual data transfers.
- Isolate VPN appliances from internal systems that do not require direct access. This will prevent lateral movement from a possible compromised edge device.
- Implement a session management policy for VPN access. This can help enforce short-lived session tokens, which can reduce the risk of session hijacking.

UNC3886

Threat Level: Medium

Attack:

UNC3886 focuses on internet-facing infrastructure, recently targeting end-of-life Juniper routers running Junos OS. These devices, commonly used by internet service providers and telecom companies, are appealing to attackers because they lack security protection and no longer receive firmware updates. UNC3886 gains initial access through stolen credentials (MITRE T1078). Once inside, the group deploys custom backdoors derived from the open-source malware TINYSHELL. The backdoors launch remote shells, disable logging, and maintain long-term access while blending in with legitimate system processes (MITRE T1036 and T1562.002). To avoid detection, the backdoor components are named to resemble legitimate Junos OS processes, allowing them to hide in plain sight. After establishing persistence, UNC3886 collects sensitive data such as logs and credentials and uses compromised routers as a starting point for lateral movement (MITRE T1570). UNC3886's activity suggests an interest not just in the devices themselves, but in using them as stealthy footholds into larger infrastructure.

Remediation:

- Identify any end-of-life or unsupported systems across the network. If possible, these devices should be retired. If they cannot be retired, they should be segmented to reduce exposure and risk.
- Establish a device lifecycle policy to ensure that end-of-life infrastructure is monitored and reviewed.
- Regularly perform threat hunting activities on network infrastructure. Use available indicators of compromise (IOCs) tied to known APT campaigns.

As stated above, threat hunting is an effective method for identifying suspicious activity in an environment. Google Mandiant is a strong source that regularly publishes IOCs linked to various threat campaigns. Below are IOCs associated with UNC5221 and UNC3886, respectively.

This IOC from Google Mandiant contains file-based indicators, such as internal code names, file hashes, filenames, and descriptions. These details help identify specific malicious files that may exist on endpoints or within environments compromised by UNC5221.

Code Family	MD5	Filename	Description
TRAILBLAZE	4628a501088c31f53b5c9ddf6788e835	/tmp/.i	In-memory dropper
BRUSHFIRE	e5192258c27e712c7acf80303e68980b	/tmp/.r	Passive backdoor
SPAWNSNARE	6e01ef1367ea81994578526b3bd331d6	/bin/dsmain	Kernel extractor & encryptor
SPAWNWAVE	ce2b6a554ae46b5eb7d79ca5e7f440da	/lib/libdsupgrade.so	Implant utility
SPAWNSLOTH	10659b392e7f5b30b375b94cae4fdca0	/tmp/.liblogblock.so	Log tampering utility

This IOC from Google Mandiant relating to UNC3886 includes network-based indicators such as IP addresses. This information can help threat hunters identify suspicious network traffic associated with UNC3886's infrastructure.

Description	Indicator
TINYSHELL Command and Control server	129.126.109.50:22
TINYSHELL Command and Control server	116.88.34.184:22
TINYSHELL Command and Control server	223.25.78.136:22
TINYSHELL Command and Control server	45.77.39.28:22
TINYSHELL Command and Control server	101.100.182.122:22
TINYSHELL Command and Control server	118.189.188.122:22
TINYSHELL Command and Control server	158.140.135.244:22
TINYSHELL Command and Control server	8.222.225.8:22

UNC5221:

- **UNC5221's Exploit Summary:** https://www.picussecurity.com/resource/blog/unc5221-cve-2025-22457-ivanti-connect-secure#who-is-the-china-nexus-group-unc5221
- **CVE-2025-22457 Vulnerability linked to UNC5221:** https://www.cybersecuritydive.com/news/cisa-ivanti-connect-secure-vulnerability-kev/744603/

UNC3886:

- **UNC3886 Exploit of Juniper Routers:** https://hackread.com/chinese-group-unc3886-backdoor-juniper-routers/
- **Technical Dive into UNC3886's Activities**: https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers

How K logix Can Help

Technology Advisory

- Email Security
- Endpoint Detection and Response (EDR)
- Identity and Access Management (IAM)
- Managed Security Service Provider (MSSP)
- Security Information and Event Management (SIEM)
- Cloud Security Posture Management (CSPM)
- SaaS Security Posture Management (SaaS)

Program Advisory

- Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
- Cloud Security Maturity
- Identity and Access Management Program Maturity

Threat Intelligence

- Notification to customers of threats
- On-demand briefings
- Threat exposure workshops
- User awareness training seminars
- Monthly and quarterly threat intelligence reports