Unveiling LIMINAL PANDA - Threats to Telecom Sector | CrowdStrike

By Counter Adversary Operations

Archived: 2026-04-05 18:26:25 UTC

On Tuesday, November 19, 2024, Adam Meyers, CrowdStrike Senior Vice President of Counter Adversary Operations, will testify in front of the U.S. Senate Judiciary Subcommittee on Privacy, Technology, and the Law on Chinese cyber threats to critical infrastructure. Within his testimony, Adam will speak publicly for the first time about a China-nexus state-sponsored actor that CrowdStrike Counter Adversary Operations tracks as LIMINAL PANDA.

Since at least 2020, LIMINAL PANDA has targeted telecommunications entities using custom tools that enable covert access, command and control (C2) and data exfiltration. The adversary demonstrates extensive knowledge of telecommunications networks, including understanding interconnections between providers. LIMINAL PANDA has used compromised telecom servers to initiate intrusions into further providers in other geographic regions.

The adversary conducts elements of their intrusion activity using protocols that support mobile telecommunications, such as emulating global system for mobile communications (GSM) protocols to enable C2, and developing tooling to retrieve mobile subscriber information, call metadata and text messages (SMS).

LIMINAL PANDA highly likely engages in targeted intrusion activity to support intelligence collection. This assessment is made with high confidence based on the adversary's identified target profile, likely mission objectives and observed tactics, techniques and procedures (TTPs) — all of which suggest long-term clandestine access requirements.

This blog provides an overview of CrowdStrike's history of tracking LIMINAL PANDA, details the adversary's key traits, targets and tactics, and recommends guidance for organizations to defend against this threat.

Tracking and Identifying LIMINAL PANDA

In 2021, CrowdStrike attributed multiple telecommunications sector intrusions to the LightBasin activity cluster, which has consistently targeted telecom entities since at least 2016 using various custom tools. An extensive review of this intrusion activity has determined some of the events documented in a previous blog post are attributable to a separate adversary now tracked as LIMINAL PANDA. This association resulted because multiple threat actors were conducting malicious activity on a highly contested compromised network.

CrowdStrike has updated the blog post to reflect activity now tracked as LIMINAL PANDA and provide additional details and TTPs, including the adversary's use of publicly available proxy tools during their intrusions. This new attribution does not impact the technical analysis regarding LightBasin's malware and TTPs described in the original analysis.

CrowdStrike continues to track all other LightBasin activity and associated malware families under the established activity cluster name. Intelligence reporting, including updates to the LightBasin operational profile, has been released to CrowdStrike Falcon® Adversary Intelligence Premium subscribers. These updates provide accurate details on the actor's target scope, TTPs and current malware attribution assessments.

LIMINAL PANDA Tools, Tactics and Behaviors

The LIMINAL PANDA adversary targets telecom providers with various tools that enable covert access, C2 and data exfiltration. In 2020 and 2021, LIMINAL PANDA likely targeted multiple telecommunications providers, using access to these entities to compromise organizations.

The adversary demonstrates extensive knowledge of telecom networks, including understanding interconnections between providers and the protocols that support mobile telecommunications. LIMINAL PANDA emulates global system for mobile communications (GSM) protocols to enable C2 and develop tooling to retrieve mobile subscriber information, call metadata and text messages.

LIMINAL PANDA employs a combination of custom malware, publicly available tools and proxy software to route C2 communications through different network segments. Table 1 lists the malware and tools associated with each actor.

LIMINAL PANDA	**LightBasin**
PingPong	*SLAPSTICK*
CordScan	*BlindingDart*
SIGTRANslator	*DaleRAT*
TinyShell (publicly available tool)	*UnimeRAT*
Fast Reverse Proxy (publicly available tool)	*DungeonKeeper*
Microsocks Proxy (publicly available tool)	*SilentKeeper*
ProxyChains (publicly available tool)	*ToxicShot*
	StealthProxy
	BridgeTroll
	cdr_xf
	sun4me
	win4me
	STEELCORGI
	LOGBLEACH

LIMINAL PANDA conducts intrusion activity that poses a significant potential threat to telecommunications entities. The adversary targets these organizations to directly collect network telemetry and subscriber information or to breach other telecommunications entities by exploiting the industry's interoperational connection requirements. LIMINAL PANDA's likely operational motivations — indicated by their development and deployment of tooling specific to telecommunications technology — closely align with signals intelligence (SIGINT) collection operations for intelligence gathering, as opposed to establishing access for financial gain.

LIMINAL PANDA has previously focused on telecommunications providers in southern Asia and Africa, suggesting that their final targets likely reside in these regions; however, individuals roaming in these areas may also be targeted depending on the compromised network's configuration and LIMINAL PANDA's current access. Equally, depending on their current collection requirements, the adversary could employ similar TTPs to target telecoms in other regions.

CrowdStrike Intelligence assesses LIMINAL PANDA's activity aligns with China-nexus cyber operations. This assessment is made with low confidence based on the following factors, which do not strongly indicate attribution on their own due to their non-exclusive nature:

- Targeting organizations operating in countries associated with China's Belt and Road Initiative (BRI), a national-level strategy seeking to establish economic opportunities aligned with Beijing's prioritized interests outlined in China's 13th and 14th Five-Year Plans.
- Using a Pinyin string (wuxianpinggu507) for *SIGTRANslator*'s XOR key and the password for some of LIMINAL PANDA's remote proxy services. This Pinyin text translates to "wireless evaluation 507" or "unlimited evaluation 507." "Wireless evaluation" is likely the correct translation, given that the malware is used to target telecommunications systems. This term is also similar to the domain wuxiapingg[.]ga, which was previously hosted on a LIMINAL PANDA-associated IP address. Several other domain names that overlap with LIMINAL PANDA's infrastructure also used Pinyin representations of Mandarin terms, further suggesting actors associated with the group's infrastructure likely speak Chinese.
- Using the domain name wuxiapingg[.]ga as delivery infrastructure and C2 for *Cobalt Strike*, a commercially available remote access tool (RAT) that China-nexus actors frequently use.
- Using *Fast Reverse Proxy* and the publicly available *TinyShell* backdoor, both of which have also been used by multiple Chinese adversaries, including SUNRISE PANDA and HORDE PANDA.
- Using VPS infrastructure supplied by Vultr, a provider commonly — albeit not exclusively — used by China-nexus adversaries and actors.

Recommendations

LIMINAL PANDA's known intrusion activity has typically abused trust relationships between telecommunications providers and gaps in security policies, allowing the adversary to access core infrastructure from external hosts.

These recommendations can be implemented to help protect against the activity described in this blog:

- Deploy an advanced, real-time endpoint protection and response (EDR) solution, such as CrowdStrike Falcon®, across the network environment, including on servers considered inaccessible from the public

internet.

- Implement complex password strategies — avoiding default or generic options — for SSH authentication or employ more secure methods such as SSH key authentication, particularly on servers that accept connections from external organizations (e.g., eDNS servers).
- Minimize the number of publicly accessible services operating on servers that accept connections from external organizations to those required for organizational interoperation.
- Enforce internal network access control policies for servers according to role and requirement (e.g., minimize opportunities for access from eDNS servers to other management devices and network infrastructure unless necessary for administration purposes); in these cases, access should be constrained by secure authentication mechanisms.
- Log SSH connections between internal servers and monitor them for anomalous activity.
- Verify `iptables` rules implemented on servers, checking for the presence of abnormal entries that enable inbound access from unknown external IP addresses.
- Employ file integrity checking mechanisms on critical system service binaries such as `iptables` to identify if they are unexpectedly modified or replaced.

CrowdStrike Intelligence Confidence Assessment

High Confidence: Judgments are based on high-quality information from multiple sources. High confidence in the quality and quantity of source information supporting a judgment does not imply that that assessment is an absolute certainty or fact. The judgment still has a marginal probability of being inaccurate.

Moderate Confidence: Judgments are based on information that is credibly sourced and plausible, but not of sufficient quantity or corroborated sufficiently to warrant a higher level of confidence. This level of confidence is used to express that judgments carry an increased probability of being incorrect until more information is available or corroborated.

Low Confidence: Judgments are made where the credibility of the source is uncertain, the information is too fragmented or poorly corroborated enough to make solid analytic inferences, or the reliability of the source is untested. Further information is needed for corroboration of the information or to fill known intelligence gaps.

Additional Resources

- *Read about the adversaries tracked by CrowdStrike Counter Adversary Operations in the CrowdStrike 2024 Threat Hunting Report.*
- *Tune into the Adversary Universe podcast, where CrowdStrike experts discuss today's threat actors — who they are, what they're after and how you can defend against them.*
- *Know the adversaries that may be targeting your region or business sector — explore the CrowdStrike Adversary Universe.*
- *Learn how CrowdStrike's threat intelligence and threat hunting solutions are transforming security operations to better protect your business.*
