LIMINAL PANDA: A Roaming Threat to Telecommunications Companies

By Jamie Harries - Dan Mayer

Archived: 2026-04-05 14:26:06 UTC

- LIMINAL PANDA has targeted telecommunications organizations in Africa and South Asia using a range of custom tools — including *SIGTRANslator*, *CordScan* and *PingPong* — while demonstrating in-depth understanding of telecommunications network architectures to laterally propagate to important systems.
- The adversary appears to have extensive knowledge of telecommunications protocols, including developing scanning and packet-capture tools to retrieve specific information (such as subscriber information and call metadata) from mobile communication infrastructure and using protocol emulators to enable command and control (C2) over infrequently monitored channels.
- The nature of the data targeted by the adversary aligns with information likely to be of significant interest to intelligence organizations and security services.
- CrowdStrike assesses LIMINAL PANDA is a targeted intrusion adversary that will likely continue targeting the telecommunications sector. This assessment is made with moderate confidence based on the adversary's demonstrated tactics, techniques and procedures (TTPs), target scope and apparent collection objectives.

The original version of this blog post — published in October 2021 — documented targeted intrusion activity against telecommunications organizations using a range of custom malware families, novel telecommunications protocol-specific command-and-control (C2) techniques, and publicly available proxy software. At the time, this activity was attributed to LightBasin, an activity cluster employing a range of custom tooling focused on targeting the telecommunications and financial sectors.

Further review of related intrusion activity determined that the operation detailed in this blog was attributed to LightBasin and is now associated with a likely China-nexus adversary dubbed LIMINAL PANDA. While this new assessment does not impact the previous technical analysis of malware and TTPs described previously, this blog post has been updated to reflect this new attribution, reflecting CrowdStrike's commitment to continually re-evaluate evidence and provide accurate reporting on adversary groups.

In addition, a new blog provides deeper insights into LIMINAL PANDA's operational profile and key TTPs, as well as guidance for organizations to defend against this sophisticated adversary.

Background

CrowdStrike Services and CrowdStrike Intelligence investigated multiple intrusions conducted by an adversary now tracked as LIMINAL PANDA.

LIMINAL PANDA primarily compromises Linux-based systems common in network environments supporting telecommunications infrastructure and only interacts with Windows hosts as needed.[1] The adversary takes advantage of server configurations that enable interoperability between telecommunications networks by using previously established access on remote providers to propagate to new target networks.

The adversary implements operations security (OPSEC) measures to hide these connections from investigators by tampering with legitimate binaries on target systems. Once LIMINAL PANDA gains access to a network, they establish multiple redundant remote access mechanisms using a combination of custom backdoors and publicly available proxy tools configured to relay traffic to adversary-controlled remote infrastructure.

GPRS eDNS Servers

LIMINAL PANDA compromised several telecommunications companies via their external DNS (eDNS) servers, which are part of the General Packet Radio Service (GPRS) network and play a role in roaming between different mobile operators.

This enabled the adversary to connect directly from other compromised telecommunication companies' GPRS networks. CrowdStrike determined LIMINAL PANDA has likely compromised at least 13 telecommunication companies across the world since at least 2019.

During the investigation, CrowdStrike uncovered evidence showing LIMINAL PANDA initially accessed the first eDNS server via SSH from another compromised telecommunications company by password spraying extremely weak and third-party-focused passwords (e.g., `huawei`).

Later, LIMINAL PANDA returned to access several eDNS servers from one of the compromised telecom entities while deploying a backdoor dubbed *PingPong* using the filename `/usr/bin/pingg`, and established persistence by modifying the SysVinit script `/etc/rc.d/init.d/sshd` to include the following line:

```
cd /usr/bin && nohup ./pingg >/dev/null 2>&1 &
```

PingPong listens for inbound magic ICMP `echo` requests and establishes a TCP reverse shell connection to an IP address and port specified at certain offsets within the packet. The `/bin/bash` process *PingPong* spawns masquerades under the process name `httpd`.

Firewalls usually protect eDNS servers from unauthorized external internet access; the magic packet that *PingPong* expects would most likely have to be sent from other compromised GPRS network infrastructure. CrowdStrike Services observed reverse shells that had been spawned from this implant that communicated with a server owned by a different compromised telecom entity in another part of the world. These connections typically communicated with the remote system on TCP port 53 — the port primarily used for DNS — further indicating the adversary's attempts to disguise their activity as legitimate traffic.

In addition to deploying the *PingPong* backdoor, LIMINAL PANDA added `iptables` rules to the eDNS server, ensuring continued SSH access to the server from five other compromised telecom entities. The adversary also replaced the legitimate `iptables` binary with a wrapper binary (SHA256 hash: `97d4c9b5750d614face73d11ba8532e53594332af53f4c07c1543195225b76eb`) that filters output from `iptables` queries, including the first two octets of remote IP addresses belonging to the compromised telecommunications companies. These actions make it more difficult for administrators and analysts to identify the firewall rules by reviewing `iptables` output alone. Indicators relating to this utility are highlighted in Table 1.

Table 1. Wrapper binaries and legitimate `iptables` file details

File Path	Description
`/usr/local/sbin/iptables`	`iptables` wrapper binary that replaced legitimate version (SHA256 hash: `97d4c9b5750d614face73d11ba8532e53594332af53f4c07c1543195225b76eb`)

`/usr/sbin/iptablesDir/iptables`
`/usr/sbin/iptablesDir/iptables-apply`
`/usr/sbin/iptablesDir/iptables-batch`
`/usr/sbin/iptablesDir/iptables-multi`
`/usr/sbin/iptablesDir/iptables-restore`
`/usr/sbin/iptablesDir/iptables-save`
	Legitimate `iptables` binaries in a non-standard directory that are invoked by the trojanized version

Serving GPRS Support Node (SGSN) Emulation

LIMINAL PANDA uses a novel technique to support C2 communication, leveraging SGSN emulation software in concert with *TinyShell*. SGSNs are essentially GPRS network access points, and the emulation software allows the adversary to tunnel traffic via this telecommunications network.

TinyShell is an open-source Unix backdoor used by multiple adversaries; however, LIMINAL PANDA uniquely combined this malware with the publicly available SGSN emulator `sgsnemu` [2] via a bash script. This script constantly runs on compromised systems but only executes certain steps between 2:15 and 2:45 UTC each day, a time window specified via command-line arguments. During the defined period, the script performs the following steps in a loop:

1. Execute *TinyShell* configured to communicate with an adversary-controlled C2 IP address hosted by the virtual private server (VPS) provider Vultr
2. Add a route to the *TinyShell* C2 on the interface `tun0`
3. Check *TinyShell* C2 connectivity via `ping`
4. If *TinyShell* fails to connect to the C2, the script executes the SGSN emulator in a loop, attempting to connect to nine pairs of International Mobile Subscriber Identity (IMSI) and Mobile Subscriber Integrated Services Digital Network (MSISDN) numbers passed as arguments to the emulator. These numbers identify specific mobile devices, or mobile stations, for the SGSN emulator to create tunnels to. This process generates Packet Data Protocol (PDP) context requests for mobile stations with the IMSI/MSISDN number pairs until a connection is established. If a connection is established, the SGSN emulator connects to the device via the GPRS Tunnelling Protocol (GTP) and uses the `tun0` interface for the connection. The *TinyShell* implant then uses `tun0`, as described previously.
5. If no connection has been made by the end of the 30-minute window, the script kills both the SGSN emulator and the *TinyShell* instance.

In summary, the SGSN emulator is used to tunnel *TinyShell* C2 traffic between the infected host and remote C2 server via GTP through specific mobile stations. The script is used as a persistence mechanism; it runs continually but attempts to establish a tunnel to each of the specified mobile stations, which act as tunnels to the *TinyShell* C2 server. The script runs for only 30 minutes each day, culminating in a similar effect to a scheduled job.

CrowdStrike Intelligence assesses that this sophisticated form of C2 is likely an OPSEC measure. This assessment is made with moderate confidence, as GTP-encapsulated *TinyShell* C2 traffic is less likely to be considered anomalous within mobile communications networks. Additionally, network security solutions are less likely to inspect and restrict GTP-encapsulated traffic.

Additional Malware and Utilities

LIMINAL PANDA has also deployed numerous custom and publicly available tools to support ongoing intrusion operations and enable reconnaissance and data collection.

CordScan

CordScan is a network-scanning and packet-capture utility containing built-in logic to fingerprint and retrieve data relating to common telecommunication protocols from infrastructure such as SGSNs. LIMINAL PANDA may target SGSNs for further collection, as this infrastructure is responsible for packet-data delivery to and from mobile stations, and also contains location information for registered GPRS users. CrowdStrike identified multiple versions of this utility, including a cross-compiled version for systems running on ARM architecture, such as Huawei's commercial CentOS-based operating system EulerOS.

LIMINAL PANDA's ability to fingerprint various brands of networking hardware and compile tools for appropriate processor architectures likely indicates the adversary's robust research and development capabilities to target vendor-specific infrastructure commonly seen in telecommunications environments. This access development effort may indicate an intelligence organization or security service collection requirements against a diverse set of target environments.

SIGTRANslator

SIGTRANslator is a Linux ELF binary capable of sending and receiving data via various SIGTRAN protocols that carry public switched telephone network (PSTN) signaling over IP networks. This signaling data includes valuable metadata such as telephone numbers called by a specific mobile station. Data collected and relayed by *SIGTRANslator* is also sent to a remote C2 host that connects to a port opened by the binary. This allows the remote C2 server to collect data proxied by *SIGTRANslator* as well as send data to the tool to be retransmitted via a SIGTRAN protocol.

SIGTRANslator traffic sent to and from the remote C2 is encrypted with the hardcoded XOR key `wuxianpinggu507`. 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. The Pinyin artifact indicates *SIGTRANslator*'s developer has some knowledge of the Chinese language.

Fast Reverse Proxy

LIMINAL PANDA uses this open-source reverse proxy to provide general access to the eDNS server via an adversary-controlled C2 IP address hosted by the VPS provider Vultr.

Microsocks Proxy

LIMINAL PANDA typically uses this open-source SOCKS5 proxy server to pivot to systems internally.

ProxyChains

This open-source utility can transmit network traffic through a chain of proxy servers, even if the program generating the traffic does not have proxy support. It uses a configuration file specifying proxy IP addresses and associated credentials to use. A recovered LIMINAL PANDA-associated *ProxyChains* configuration file contained a mixture of local IP addresses, IP addresses assigned to Vultr, and IP addresses belonging to eight different telecommunication organizations across the globe.

Recommendations

Telecommunications servers must communicate with one another as part of cellular roaming agreements between providers; however, LIMINAL PANDA's ability to pivot between multiple networks is enabled by overly permissive access policies that are not restricted to required services and protocols. As such, telecom entities should ensure that firewalls protecting GPRS network borders restrict network traffic to necessary protocols such as DNS or GTP.

As LIMINAL PANDA can conduct C2 over common telecommunications protocols, organizations compromised by the adversary are likely unable to remediate intrusions by solely restricting network traffic. In this event, CrowdStrike recommends conducting an incident response investigation that reviews all partner systems alongside all systems managed by the organization itself. This recommendation also applies to any organization seeking to determine whether LIMINAL PANDA has compromised their system.

If any aspects of a telecom entity's network are managed by a third-party managed service provider (MSP), organizations should evaluate the partner's security controls to ensure systems are sufficiently protected. CrowdStrike Services investigations commonly reveal a lack of any monitoring or security tooling on core telecommunication network systems.

While the security tooling is infrequently applied to real-time operating systems, LIMINAL PANDA typically targets other Unix-based operating systems that support core telecommunications network services and should have basic security controls and logging in place such as:

- SSH logging forwarded to a SIEM
- Endpoint detection and response (EDR) for process execution
- File integrity monitoring (FIM) for recording file changes of key configuration files

Additionally, organizations should implement appropriate incident response plans that account for partner-managed systems within the network. This incident response plan enumerates the roles and responsibilities of third-party MSPs to ensure forensic artifacts can be acquired from third-party equipment not managed by the telecom.

Finally, given that highly advanced state-sponsored adversaries consistently target telecoms, these organizations must have access to up-to-date and comprehensive threat intelligence resources to understand the threats facing the industry. This intelligence should also provide insights into the TTPs of adversaries that typically target telecoms — both corporate networks and critical telecommunications infrastructure — and allow telecoms to further augment detection mechanisms and evaluate existing security controls.

Conclusion

Because telecommunications entities possess information with significant intelligence value, CrowdStrike assesses that sophisticated adversaries will continue to target telecoms and their constituent infrastructure. While the partner-heavy nature and high-availability systems associated with these networks make implementing robust cybersecurity a complex task, securing all aspects of telecommunications infrastructure — not only the corporate network — is crucial.

Indicators of Compromise

Table 2. LIMINAL PANDA indicators of compromise

Indicator	SHA256 Hashes	Descrip
`/usr/bin/pingg`	`e9c0f00c34dcd28fc3cc53c9496bff863b81b06723145e106ab7016c66581f72` `4668561d60daeb7a4a50a9c3e210a4343f92cadbf2d52caab5684440da6bf562`	*PingPo* backdo
`/usr/lib/om_proc`	`3a259ad7e5c19a782f7736b5ac50aac4ba4d03b921ffc6a3ff6a48d720f02012` `65143ccb5a955a22d6004033d073ecb49eba9227237a46929495246e36eff8e1`	*Microsc Proxy* (tool)
`/usr/lib/frpc`	`05537c1c4e29db76a24320fb7cb80b189860389cdb16a9dbeb0c8d30d9b37006` `16294086be1cc853f75e864a405f31e2da621cb9d6a59f2a71a2fca4e268b6c2`	*Fast Re Proxy* (tool)
`/usr/lib/frpc.ini`	`N/A`	*Fast Re Proxy* configu file nam

`/usr/lib/cord.lib`
`/usr/lib/libcord.so`
`/usr/bin/libcord.so`
	`6d3759b3621f3e4791ebcd28e6ea60ce7e64468df24cf6fddf8efb544ab5aec0`
	`c5ddd616e127df91418aeaa595ac7cd266ffc99b2683332e0f112043796ede1d`
	`9973edfef797db84cd17300b53a7a35d1207d166af9752b3f35c72b4df9a98bc`
	`4480b58979cc913c27673b2f681335deb1627e9ba95073a941f4cd6d6bcd6181`
	`ad9fef1b86b57a504cfa1cfbda2e2ac509750035bff54e1ca06f7ff311d94689`
		CordSc

`/home/REDACTED/cordscan_raw_arm`	`cdf230a7e05c725a98ce95ad8f3e2155082d5a6b1e839c2b2653c3754f06c2e7`	*CordSc* (ARM architec
`/usr/lib/javacee`	`917495c2fd919d4d4baa2f8a3791bcfd58d605ee457a81feb52bc65eb706fd62`	*SIGTRA*
`/usr/lib/sgsnemu` `/usr/bin/sgsnemu`	`bf5806cebc5d1a042f87abadf686fb623613ed33591df1a944b5e7879fb189c8` `78c579319734a81c0e6d08f1b9ac59366229f1256a0b0d5661763f6931c3b63c`	SGSN emulato (public

`/usr/lib/sgsnemu_bak`	`b06f52e2179ec9334f8a3fe915d263180e538f7a2a5cb6ad8d60f045789123b6`	
`/usr/lib/tshd`	`a388e2ac588be6ab73d7e7bbb61d83a5e3a1f80bf6a326f42b6b5095a2f35df3`	*TinyShe* (public
`/home/REDACTED/win7_exp/proxychains.conf` `/usr/lib/win7_exp/proxychains.conf`	`N/A`	*ProxyCl* configu file nam
`/usr/local/sbin/iptables`	`97d4c9b5750d614face73d11ba8532e53594332af53f4c07c1543195225b76eb`	`iptabl` wrapper
`/usr/sbin/iptablesDir/` `/sbin/iptablesDir/`	`N/A`	Adversa created director containi legitima copies c iptables binaries by the `iptabl` wrapper
`45.76.215[.]0/24`	`N/A`	Vultr IP address used by LIMIN/ PANDA
`167.179.91[.]0/24`	`N/A`	Vultr IP address used by LIMIN/ PANDA
`45.32.116[.]0/24`	`N/A`	Vultr IP address used by LIMIN/ PANDA
`207.148.24[.]0/24`	`N/A`	Vultr IP address used by LIMIN/ PANDA
`172.104.79[.]0/24`	`N/A`	Linode address used by LIMIN/ PANDA

`45.33.77[.]0/24`	`N/A`	Linode address used by LIMIN/ PANDA
`139.162.156[.]0/24`	`N/A`	Linode address used by LIMIN/ PANDA
`172.104.236[.]0/24`	`N/A`	Linode address used by LIMIN/ PANDA
`172.104.129[.]0/24`	`N/A`	Linode address used by LIMIN/ PANDA

Endnotes

1. Key examples of telecommunications-specific systems targeted include systems involved in the GPRS network such as external DNS (eDNS) servers, Service Delivery Platform (SDP) systems, and SIM/IMEI provisioning, as well as Operations Support Systems (OSS) and Operation and Maintenance Units (OMU).
2. https[:]//osmocom[.]org/projects/openggsn/wiki/Sgsnemu

CrowdStrike Intelligence Confidence

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.*
