Three China-Nexus Espionage Clusters Linked Through Shared Sparrow Malware Ecosystem



Check Point Research reports three activity clusters sharing infrastructure and malware code similarities, targeting telecoms, government, military, research and critical infrastructure across Latin America, Asia and Europe over the past year.

- Three distinct activity clusters share infrastructure and malware code similarities.
- Check Point Research is tracking them; one cluster name given in the source is SilentDelivery.
- Targets include telecoms, government, military, research institutions and critical infrastructure.
- Activity was observed over the past year across Latin America, Asia and Europe.
- The source describes the campaigns as China-nexus espionage linked through the Sparrow malware ecosystem.

Check Point Research has described three separate threat activity clusters that, despite being tracked individually, share infrastructure and show similarities in malware code. The source links them through a common malware ecosystem called Sparrow and characterises the activity as China-nexus espionage.

What was observed

Over the past year, the clusters targeted telecommunications providers, government organizations, military entities, research institutions and critical infrastructure. The reported geography is Latin America, Asia and Europe. One of the cluster names given in the source is SilentDelivery; the available excerpt does not list the others or give technical detail such as initial access methods, indicators or affected products.

Why it matters for the Kingdom

The targeted sectors overlap closely with those regulated in Saudi Arabia, particularly telecommunications, government and critical infrastructure. The source does not report any activity in the Kingdom or the wider Gulf, so this is a matter of awareness and readiness rather than a confirmed local incident. Shared infrastructure across clusters also means that intelligence on one set of indicators may help detect related activity.

Institutions should review the full Check Point Research publication for indicators and techniques, and use it to test existing detection and response arrangements.

What to do now

1. Obtain the full Check Point Research report and extract published indicators and techniques.
2. Search historical logs and threat-hunt for the published indicators, prioritising telecom, government-facing and critical systems.
3. Validate that threat-intelligence feeds used by your SOC cover the Sparrow ecosystem and the named clusters.
4. Review segmentation and privileged-access controls around critical infrastructure and research environments.
5. Confirm incident escalation paths, including notification to the National Cybersecurity Authority where required.