DARKTRACE

Crimson Echo: Takeaways for CISOs and SOC Leaders

Darktrace's Chinese-nexus investigative report, "Crimson Echo: Understanding Chinese-nexus Cyber Tradecraft Through Behavioral Analysis," is based on a long-term review and threat hunt for evidence of cybersecurity incidents involving Chinese-nexus threat actors across the customer base since mid-2022.

Chinese-nexus operations have evolved beyond opportunistic intrusions and now reflect:

- Strategic, geopolitical prioritization, particularly around critical national infrastructure (CNI), dual-use industrial sectors, and regions aligned to China's global objectives.
- Operational bifurcation, where threat actors pursue either rapid "smash and grab" compromises or prolonged "low and slow", multistage intrusions focused on persistent access and espionage.
- Advanced TTPs that evade signature-based detection, including exploitation of internet-facing systems, DLL side loading, DNS tunnelling, cloud-hosted tooling, ORB networks, and living-off-the-land techniques

The findings of this report reveal how exact distinctions between Chinese-nexus subgroups are not directly necessary for effective defense against such threats. This work is not about novelty of individual findings; it's about whether the industry has correctly internalized what those findings imply when viewed over time.

Organizations with increased risks of being targeted should consider tailoring their security controls, SOC directives, and threat hunting efforts to address the challenges posed by such groups while also reshaping their readiness, investments, and resilience planning for the next phase of state-aligned offensive cyber activity.

Targeting Trends and Distribution

China has evolved into one of the most prolific and capable global cyber powers. Its offensive cyber posture services multiple objectives (outlined below), a finding echoed across assessments from the Office of the Director of National Intelligence (ODNI), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency, the Federal Bureau of Investigation, and Five Eyes [1].

- Long term economic advantage through industrial espionage.
- Global supply-chain positioning via access to logistics, manufacturing, and digital infrastructure.
- Preparation for geopolitical flashpoints, particularly involving Taiwan and South China Sea.

Across cases confirmed by Darktrace, Chinese-nexus targeting strongly correlated with the target's strategic, economic, or geopolitical value. The vast majority of cases (88%) were observed in critical national infrastructure sectors. Top targeted sectors include:

- Transportation systems (e.g., aviation, rail, maritime, port authorities)
- Digital communications & telecommunications
- Critical manufacturing (e.g., industrial machinery, high-tech materials, advanced electronics)
- Healthcare & biomedical research
- Information Technology (IT) & cloud services
- Public sector and Defense Industrial Base (DIB)

The concentration around sectors with core economic and operational dependencies indicates a deliberate strategy to expand China's influence across key global leverage points [2].

Nearly a quarter (22.5%) of observed cases occurred in the US, surpassing any other country or region by far with a strong focus on critical national infrastructure and high value technology sectors. This reflects the strategic rivalry between the two nations and the intelligence need for logistics readiness, innovation, and defense adjacent capabilities.

EMEA-based intrusions had an emphasis on manufacturing, logistics, telecommunications, and energy. Three of the top five countries most observed were EU states. More specifically, targeting of the German manufacturing sector, Italian defense and IT sectors, and French retail sector were noteworthy given the significant share of each country's Gross Domestic Product (GDP) they represent.

In the Asia-Pacific and Japan (APJ) region, a balanced distribution with heavy focus on public sector and communication providers was observed alongside intrusions in government that typically occurred in the run up to strategic diplomatic meetings.

Across regions, the targeting patterns map to China's security priorities, industrial ambition, and geopolitical positioning.

Two Operational Models of Chinese-Nexus Intrusions

Chinese-nexus actors show a reliance on several key tactics, techniques, and procedures (TTPs) that should frame detection and response heuristics, including:

- Internet-facing device exploitation remains a core initial access vector for such groups, appearing in 63% of cases observed, and therefore warrants more proactive patch management and monitoring for these systems.
- Utilization of binaries native to an organization's networks and preexisting remote management tools for lateral movement, and authorized application protocols for outbound traffic for command-and-control (C2) activities appear commonly.
- Evasive techniques such as DLL side loading and reliance on anonymizing infrastructure are most commonly observed.

IT leaders can respond by more closely tracking authorized use of specific management software and associated privileges, as well as more closely monitoring DNS, TLS, and HTTP traffic for tunnelling and C2 activities. Incorporating anomaly-based detection methods and tooling can also better address these challenges.

Chinese-nexus compromises more commonly feature quick, short duration operations, while a smaller subset of cases include long-term persistence. The median compromise duration of around 10 days contrasts distinctly with outlier cases lasting nearly two years.

This trend is also consistent when assessing duration until exfiltration. Cases featuring exfiltration had median time of 48 hours until egress from initial access, but an average duration of 35 days.

As such, more generalized, opportunistic compromises as well as "smash-and-grab" style attacks appear more common. Such activities may align more with broader botnet creations and proliferation of Chinese-nexus footprint in adversarial cyberspace. However, customers in sectors with higher strategic value are more likely to face longer persistence and extended compromise and egress activities ("low and slow" model).

IT leaders can use this information to prioritize Data Loss Prevention (DLP) tools, and more proactively control for outbound data flows should exfiltration be a more likely goal for threat actors on the network. Moreover, duration and tactic dwell time can better inform threat hunting parameters and timelines. Incorporation of generalized models for Chinese state-sponsored activity and a anomaly-based detection mechanism will serve leaders effectively in the near term as well to address these risks.

DOWNLOAD THE FULL REPORT ↗

References

[1] Federal Bureau of Investigation. The China Threat. Accessed 2026. https://www.fbi.gov/investigate/counterintelligence/the-china-threat

[2] Center for Strategic and International Studies. China's Weaponization of Global Cyber Supply Chains. Accessed 2026. https://www.csis.org/blogs/strategic-technologies-blog/chinas-weaponization-global-cyber-supply-chains

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,300 employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.