ultraviolet

THREAT ADVISORY

PRC-Nexus Dwell Time Statistics

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
June 3, 2026
TLP:GREEN

Executive Snapshot

China-nexus threat actors are conducting long-duration intrusions into critical infrastructure networks with the explicit objective of pre-positioning for disruptive operations during a future geopolitical crisis. These operations rely on stolen credentials, native operating system tools, and compromised edge devices to maintain access that blends with legitimate administrative activity, resulting in dwell times that routinely exceed months and in some confirmed cases stretch to years. The threat is active, ongoing, and assessed by U.S. and allied intelligence agencies as directly tied to military contingency planning around Taiwan. Organizations in the communications, energy, water, transportation, and defense industrial base sectors should treat this as a present-tense risk requiring immediate action.

- Build and maintain a complete asset inventory that includes all network edge devices, SOHO routers, VPN concentrators, firewalls, and end-of-life equipment. Each device should have a documented owner, a current firmware version recorded against the vendor's latest supported release, and a defined lifecycle status. Devices that have reached end-of-life or end-of-support should be flagged for replacement on a defined timeline, as these are the primary footholds China-nexus actors exploit for long-term persistent access.

- Establish a quarterly review cycle for all privileged and service account credentials, including a full audit of where each account authenticates, what systems it has access to, and whether its permissions still align with a documented business justification. Disable or rotate any accounts that cannot be tied to an active owner or function, and enforce multi-factor authentication on all remote access and administrative interfaces without exception.

- Document and validate all authorized communication paths between IT and OT network segments, maintaining a current network architecture diagram that reflects actual traffic flows rather than intended design. On a quarterly basis, review firewall rules, DMZ configurations, and access control lists governing the IT-to-OT boundary to confirm that no unauthorized paths have been introduced through configuration drift, vendor maintenance, or undocumented integrations.

- Implement a patching and configuration management program with defined SLAs for public-facing devices, prioritizing internet-exposed assets such as VPN gateways, remote access portals, and web application firewalls. Track patch compliance as a standing metric reported to security leadership on a monthly basis, with any public-facing device exceeding its SLA escalated for executive visibility. Known exploited vulnerabilities cataloged by CISA should be treated as critical regardless of CVSS score and patched within the agency's recommended timelines.

TIDE Team Analysis

China-nexus advanced persistent threat groups continue to represent the most significant and sustained cyber threat to Western critical infrastructure. The operational posture observed across multiple tracked clusters in 2026 confirms that these actors are not conducting traditional espionage. U.S. intelligence agencies, CISA, the NSA, and Five Eyes partners collectively assess that groups such as Volt Typhoon are pre-positioning themselves inside information technology networks to enable lateral movement to operational technology assets for the purpose of disruption or destruction during a future geopolitical crisis. This assessment is reinforced by the targeting profile itself: the networks compromised by Volt Typhoon offer minimal foreign intelligence value, the actors have prioritized the collection of network diagrams and OT system manuals, and the geographic concentration of activity around Guam and U.S. Pacific infrastructure aligns directly with military contingency planning for a Taiwan scenario. The 2025 Department of Defense China Military Power Report concludes that by 2027, the PLA expects to hold capabilities sufficient to prevail in a Taiwan conflict, and that China is actively compromising and pre-positioning within U.S. space and defense networks to disable or disrupt those systems during a conflict.

The dwell time data paints a picture that should concern any organization within the targeting aperture of these actors. Industry incident response data for 2026 places global median dwell time at 14 days, but for cyber espionage incidents specifically, that figure rises to 122 days. Even this median conceals the true distribution. A separate April 2026 analysis of China-nexus intrusions found that while the median sits around 10 days, the long tail stretches beyond 600 days, with persistence applied selectively based on target value. The concrete cases are consistent with these findings: threat intelligence reporting has documented Volt Typhoon maintaining undetected access for up to five years in some victim environments, at least one major telecom confirmed that Salt Typhoon persisted inside its network for three years prior to discovery, and Chinese actors dwelled inside the U.S. electric grid for 300 days in 2023 before the compromise was identified. The FBI confirmed in February 2026 that Salt Typhoon threats remain active and ongoing, and a separate China-linked campaign struck more than 50 telecoms and government agencies across 42 countries earlier this year.

The pre-positioning model fundamentally changes how defenders must think about the threat. Traditional espionage actors generate detectable activity through data collection and exfiltration. Pre-positioning actors, by contrast, may sit inside a network for months or years with no intent to steal data or cause disruption in the near term. Their objective is to ensure that access remains viable and that they understand the network topology well enough to execute disruptive operations on command. CISA's advisory on Volt Typhoon documents the operational sequence in detail: extensive pre-compromise reconnaissance of the target's architecture, security measures, and staff; exploitation of unpatched public-facing devices such as firewalls, routers, and VPN concentrators; credential harvesting followed by lateral movement using valid administrator accounts; and persistent access maintained across network boundaries for years. In some cases, Volt Typhoon actors abstained from using compromised credentials outside of normal working hours to avoid triggering anomaly-based alerts, demonstrating a level of operational discipline that defeats simple behavioral rules.

The tradecraft employed to sustain these long-dwell operations is deliberately designed to evade conventional detection stacks. Volt Typhoon relies almost exclusively on living-off-the-land techniques, using native operating system tools such as PowerShell, wmic, netsh, and ntdsutil rather than deploying custom malware. Recent 2026 incident response research found that identity weaknesses played a material role in nearly 90 percent of APT investigations, with 65 percent of initial access being identity-driven, meaning the initial foothold often looks indistinguishable from a legitimate login. The supporting infrastructure compounds the problem: the April 2026 joint advisory from CISA, NCSC, NSA, and ASD confirmed that China-nexus actors now route operations through large-scale covert networks of compromised SOHO routers and IoT devices that are constantly rotated, rendering static IP blocklists ineffective. Earlier industry research on IOC Extinction documented this phenomenon, and the NCSC

advisory reinforced it, noting that a single covert network may be shared across multiple actor groups simultaneously.

The IT-to-OT boundary is the critical threshold that separates pre-positioning from activation. CISA and partner agencies assess with high confidence that Volt Typhoon actors are positioning on IT networks specifically to enable lateral movement to OT assets that control physical processes in energy, water, transportation, and communications systems. A 2023 compromise of a municipal electric and water utility illustrates the pattern: the attackers entered through an unpatched next-generation firewall, then used legitimate credentials and native tools to move laterally across both IT and OT networks. Subsequent investigation found evidence of the group quietly mapping network dependencies and stealing operational data over a period of months. A 2019 vulnerability assessment of industrial control systems found that nine percent of identified vulnerabilities enabled unencumbered lateral movement from IT to OT, and many of those gaps persist in environments that lack the budget or staffing to remediate them. The convergence of limited OT visibility, legacy equipment without standard logging capabilities, and weak segmentation creates an environment where pre-positioned access can persist indefinitely.

The strategic implications extend beyond individual organizations. Taiwan's National Security Bureau reported over 960 million intrusions against the island's networks in 2025, including a greater than 1,000 percent increase in attacks against energy facilities and a 54 percent increase against hospitals and emergency services. Chinese cyber activity against the transportation sector has expanded significantly, with Volt Typhoon and associated actors observed accessing rail signaling and port operations in Guam as part of a broader campaign against U.S. Pacific logistics infrastructure. The ODNI's 2026 Annual Threat Assessment identifies PRC-linked actors as the most persistent cyber threat to U.S. government, private sector, and critical infrastructure networks. The operational picture that emerges is one of systematic preparation across all 16 critical infrastructure sectors, with the objective of holding at risk the civilian systems upon which military mobilization and societal stability depend.

For detection and hunting purposes, organizations must shift from IOC-driven approaches to behavioral and TTP-based analytics that can surface activity across extended time windows. CISA explicitly recommends that defenders assume significant dwell time and prioritize the review of application event logs, which persist on endpoints longer than security event logs and other ephemeral artifacts. Practical hunting priorities include retrospective analysis of credential access anomalies across the full log retention window, stacked analytics for LOLBin execution chains where individual events appear benign but the combination is anomalous, integrity auditing of edge devices and network infrastructure for unexpected configuration changes or enabled services, monitoring for traffic crossing IT-OT segmentation boundaries outside of documented integration points, and detection of reconnaissance activity targeting internal documentation repositories containing network diagrams or OT system manuals. For organizations operating OT environments where standard logging is unavailable, CISA recommends collecting network traffic between OT assets and implementing file integrity monitoring to detect unauthorized changes.

The recommended organizational response is threefold. First, execute a comprehensive threat hunt against the maximum available log retention window, specifically targeting the persistence and lateral movement techniques documented in CISA Advisory AA24-038A and the April 2026 covert networks advisory AA26-113A. Second, convert hunt findings into persistent detection analytics that run continuously in the SIEM and EDR stack, with quarterly refresh cycles informed by updated China-nexus reporting. Third, conduct red team exercises that specifically simulate the pre-positioning kill chain: valid credential acquisition, LOTL lateral movement across IT subnets, and boundary crossing into OT networks without data exfiltration. The objective of these exercises is to validate whether existing detection coverage would identify an actor whose behavior closely mirrors legitimate administrative activity and whose intent is to maintain quiet, long-term access rather than achieve an immediately visible objective. The threat is not theoretical. These actors are inside networks today, and the question facing defenders is whether their detection capabilities are calibrated to find activity that is designed to look like nothing at all.

Why It Matters

The China-nexus threat actors operating today are not the same actors that defenders confronted a decade ago. Earlier Chinese cyber campaigns were frequently characterized by large-scale, relatively noisy operations that relied on custom malware families and command-and-control infrastructure that defenders could signature and block. The operational security failures of that era led to high-profile indictments, public attributions, and eventually a wholesale recalibration of tradecraft. The current generation has absorbed those lessons. These groups now use valid credentials as their primary access mechanism, execute operations almost entirely through native operating system tools, route traffic through massive botnets of compromised consumer devices, and deliberately target infrastructure components that sit outside the visibility of modern endpoint security platforms. The result is an operational model engineered from the ground up to extend dwell time rather than accept the compression that the rest of the threat landscape has experienced. Frontline reporting from 2026 also documents that exploitation of vulnerabilities is now routinely occurring before a patch is even released, which means that espionage actors combining rapid exploitation with patient, tool-free persistence can establish initial access that may never generate a signature-based alert at any point in the intrusion lifecycle.

The industry's most widely cited dwell time benchmarks obscure this reality. Over the past decade, global median dwell time has dropped dramatically, falling from well over a year to roughly two weeks. That trajectory appears to reflect extraordinary defensive progress, but the decline has been driven largely by the explosion of ransomware, where the attacker's economic model depends on rapid detonation rather than sustained access. As ransomware cases have come to dominate incident response caseloads, they have pulled the aggregate median downward, creating a statistical illusion. At the other end of the distribution, espionage actors are moving in the opposite direction. The 2026 data shows espionage-specific dwell times averaging four months, and confirmed China-nexus intrusions have stretched to five years in some environments. The headline metric is improving, but the threat that matters most to critical infrastructure organizations is getting harder to find, not easier.

This divergence is projected to widen. Ransomware operators will continue compressing their timelines because speed is their competitive advantage and improving detection capabilities are forcing them to move faster. China-nexus actors will continue extending theirs because patience is their competitive advantage and the strategic value of pre-positioned access increases the longer it remains undetected. For defenders, this means that the same organization may need to maintain two fundamentally different security postures simultaneously: one built for the rapid kill chains of financially motivated intrusions measured in hours, and another built for the slow, methodical expansion of state-sponsored actors measured in months and years. The organizations most at risk are those that have invested heavily in the first posture while assuming the declining global median means the second is no longer a priority. The consequences of that miscalculation are not limited to data loss. They extend to the potential disruption of physical infrastructure during a geopolitical crisis in which there will be no time to remediate.

How to Respond

- Strictly adhere to cybersecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Remove default credentials and disable unnecessary management services on all edge network devices, including SOHO routers and firewalls, and confirm configurations against a documented hardening baseline.
- Schedule a quarterly review of firewall rules and access control lists governing critical network boundaries, with sign-off from both IT operations and security leadership.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a Red Team or Purple Team engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Conducting hypothesis driven threat hunts across the maximum available log retention window, focusing on credential access anomalies, LOLBin execution chains, and any authentication activity that deviates from established behavioral baselines for service and privileged accounts. UVCyber customers will be informed of the results through secure channels.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---