SECURITY ADVISORY

CYBER STASH

December, 2025

BRICKSTORM: Beneath the Security Stack

Context

BRICKSTORM represents a mature and strategically significant cyber-espionage capability operated by a China-nexus threat actor assessed to be aligned with long-term state intelligence objectives. Over multiple investigation cycles spanning more than a year, BRICKSTORM has demonstrated persistent evolution, environmental adaptability, and a clear operational focus on strategic access rather than short-term disruption.

Unlike commodity malware or financially driven campaigns, BRICKSTORM is purpose-built for long-dwell espionage operations. Its deployment is tightly coupled with intrusion activity that prioritises stealth, persistence, and selective data access over speed or scale. The malware has been observed evolving across successive reporting periods, reinforcing the assessment that it is actively maintained and operationally important to its operators.

What distinguishes BRICKSTORM is not merely its technical sophistication, but where it is deployed. Rather than relying solely on traditional workstation or server footprints, BRICKSTORM has been systematically positioned within virtualisation platforms, identity infrastructure, and cloud-adjacent environments—areas that often sit outside the primary visibility of conventional endpoint security tooling. This placement enables lateral reach across entire environments while remaining largely invisible to standard security controls.

The cumulative reporting over the past year reveals a consistent picture: BRICKSTORM is being used as an access-enabling platform—a strategic foothold that supports broader cyber-espionage missions such as long-term collection, target network mapping, credential harvesting, and downstream exploitation. Its repeated appearance across separate investigations, timeframes, and regions indicates an organised, well-resourced adversary with operational continuity rather than opportunistic activity.

From an intelligence perspective, BRICKSTORM should be viewed not as a standalone piece of malware, but as a core component of a wider covert access framework supporting Chinese state-aligned cyber operations. Its continued refinement across successive campaigns, combined with disciplined operational security, reflects an adversary that is investing in enduring, low-visibility access rather than short-term operational gains. This approach prioritises deniability, long-dwell persistence, and future-option access, enabling strategic leverage to be exercised at a time of the adversary's choosing.

This report provides a strategic, multi-source intelligence assessment of the BRICKSTORM campaign, translating technical tradecraft into executive-level risk, intent, and defensive priorities for organisations and national stakeholders.

Who BRICKSTORM Hunts

BRICKSTORM is not deployed at random. Its victim profile reflects deliberate target selection aligned with strategic intelligence collection and indirect access into wider ecosystems, rather than opportunistic compromise or mass exploitation.

Across all observed activity, the dominant targeting theme is organisations that act as intelligence multipliers—entities whose networks, data holdings, or trusted access provide visibility into dozens or even hundreds of downstream environments. This includes technology service providers, cloud and managed service operators, professional services firms, and organisations operating critical digital infrastructure.

A consistent characteristic of BRICKSTORM targeting is its focus on control planes rather than end-user devices. Instead of pursuing individual workstations, the malware is positioned where it can observe, influence, or traverse entire environments—identity systems, virtualisation management layers, authentication services, and core administrative platforms. This enables a single successful deployment of BRICKSTORM to yield persistent access across a large and strategically valuable attack surface.

Both public and private sector entities have been affected. Government bodies, regulatory agencies, and policy-adjacent organisations are targeted for their geopolitical intelligence value, while commercial enterprises—particularly within legal, technology, data services, and telecommunications sectors—are pursued for their intellectual property, client data, and trusted network access.

Geographically, targeting reflects a broad global intelligence requirement rather than a regional campaign. Victims span North America, Europe, and the Indo-Pacific, with no evidence of financially motivated filtering or ransomware-style victim economics. Instead, selection is driven by strategic relevance, network position, and access leverage.

In practical terms, BRICKSTORM's targeting model reveals an adversary that values who an organisation connects to as much as the organisation itself. The true objective is often not the immediate victim, but the privileged pathways that victim provides into partner networks, government systems, or high-value commercial ecosystems.

The Mechanics of Silent Access

BRICKSTORM is engineered for control without detection. Its tradecraft reflects an adversary that values operational security, patience, and long-term access over rapid impact or visible disruption. Every aspect of its use is designed to blend into normal infrastructure operations while quietly extending the attacker’s reach.

At a high level, BRICKSTORM operations follow a “low-friction, high-leverage” model. Initial intrusions focus on environments that naturally sit at the centre of enterprise trust and visibility—virtualisation platforms, identity systems, and management interfaces that govern large portions of an organisation’s digital estate. By embedding itself at these layers, BRICKSTORM achieves disproportionate access with minimal operational footprint.

Once established, BRICKSTORM is used as a persistent access broker rather than a traditional command-and-control implant. It enables discreet interactive access, lateral movement staging, credential discovery, and network mapping, all while avoiding patterns commonly associated with noisy post-exploitation tools. Its functionality supports both hands-on-keyboard espionage and automated background collection.

A defining feature of BRICKSTORM tradecraft is its deliberate positioning outside the visibility boundary of most security control stacks. By operating on infrastructure layers that are often weakly monitored—such as hypervisors, administrative platforms, and hybrid cloud connectors—the malware sidesteps the detection logic that typically protects endpoints and user workloads. This produces an asymmetric advantage: defenders may believe core systems are secure while adversaries maintain uninterrupted access beneath them.

Operational communications and access channels are equally disciplined. BRICKSTORM activity is characterised by layered obfuscation, proxying, and encrypted transport, complicating attribution, traffic inspection, and sinkholing efforts. Rather than relying on static infrastructure, the operators favour flexible, professionally managed routing that allows rapid reconfiguration without destabilising established access.

Perhaps most notable is what BRICKSTORM does not do. It does not encrypt environments, deface systems, or generate overt signals of compromise. There is no monetisation pressure, no extortion, and no visible destructive intent. Its entire operational design points to a single objective: to remain present, unseen, and prepared.

In strategic terms, BRICKSTORM is best understood as a covert access framework embedded inside critical digital arteries. It does not merely support intrusion—it enables sustained surveillance, strategic credential capture, and future-option exploitation across complex, interconnected enterprise and government networks.

Risk Mitigation

Overview

BRICKSTORM signals a structural shift in modern cyber-espionage tradecraft. Advanced adversaries are no longer constrained to endpoints and traditional servers; they are now deliberately embedding themselves within virtualisation platforms, identity systems, network appliances, and cloud control layers—the very foundations that govern enterprise trust and access. These layers typically sit outside the visibility of standard EDR tooling and default SIEM alerting, creating a silent zone of systemic risk.

This reality forces organisations to fundamentally reassess their security posture. Endpoint-centric security models are no longer sufficient against actors like BRICKSTORM. Effective defence now demands a tightly integrated blend of preventive and detective controls purpose-built to protect non-traditional operating environments—including management planes, identity infrastructure, and core platform services that, if compromised, grant disproportionate control over entire enterprises.

BRICKSTORM’s most dangerous attribute is therefore not just how it operates, but where it chooses to persist. By establishing itself at the infrastructure and identity strata, BRICKSTORM effectively operates beneath the defender’s security stack, bypassing many of the controls organisations rely upon for detection and response. This architectural positioning is fundamentally different from typical endpoint-centric APT campaigns and represents a far more systemic and enduring form of compromise.

The risk mitigation strategies that follow are designed to support a necessary shift in defensive thinking: away from dependence on default alerts, and toward a deliberate, risk-driven security model that anticipates control-plane abuse, enforces independent visibility across under-monitored systems, and hardens the full digital estate against long-dwell, infrastructure-level intrusion.

Strategic Risk Mitigation

#	Strategy	Purpose	Executive Outcome
1	**Control-Plane Zero Trust**	Treat virtualisation platforms, identity systems, appliances, and cloud management layers as Tier-0 assets with zero implicit trust	Prevents systemic takeover from a single infrastructure compromise
2	**Independent Infrastructure Telemetry**	Deploy logging and behavioural monitoring outside EDR and default SIEM for hypervisors, identity services, and appliances	Eliminates blind spots where BRICKSTORM-class threats operate
3	**Privileged Identity Containment**	Enforce MFA everywhere, PAM, and removal of standing privileged access across all control-plane identities	Disrupts the primary attack surface used for persistent access
4	**Infrastructure Egress Control**	Default-deny outbound internet access from hypervisors, management servers, and identity platforms	Breaks covert control and command channels at the infrastructure layer
5	**Assume-Compromise for Tier-0 Systems**	Continuous integrity monitoring, proactive hunting, and rapid rebuild capability for control-plane assets	Ensures resilience against long-dwell and stealth persistence

Strategic Motivation

BRICKSTORM is best understood not as an isolated malware operation, but as a state-aligned capability designed to enable long-term strategic intelligence collection and access positioning. Its tradecraft, target selection, and persistence model align closely with national cyber-espionage objectives rather than criminal monetisation or short-term operational gain.

At its core, BRICKSTORM supports a strategy of strategic access pre-positioning. By embedding itself within virtualisation platforms, identity infrastructure, and cloud control layers, the adversary establishes durable footholds that can be leveraged for intelligence collection today and operational leverage in the future. This approach creates latent access—quietly maintained pathways that can be activated at a time of the attacker's choosing, including during periods of heightened geopolitical tension.

The focus on technology providers, service firms, government-adjacent entities, and control-plane infrastructure reflects a clear intent to maximise information asymmetry. Rather than targeting isolated organisations for discrete data theft, BRICKSTORM enables the compromise of ecosystems—allowing visibility into communications, authentication flows, intellectual property, legal strategy, and the trusted relationships that underpin governments and critical industries.

This activity aligns with broader state objectives centred on:

- Persistent intelligence dominance across diplomatic, defence, economic and technological domains
- Supply-chain and downstream access leverage, where one compromise provides access to many
- Strategic preparation for future conflict, where infrastructure-level access becomes a national power enabler
- Long-term erosion of adversary confidentiality rather than immediate operational disruption

Notably, BRICKSTORM's operational design avoids the hallmarks of financially motivated or disruptive campaigns. There is no extortion pressure, no destructive signalling, and no incentive for rapid exposure. Instead, its disciplined stealth, infrastructure-level positioning, and prolonged dwell times point to a singular purpose: to remain inside strategic networks for as long as possible, unseen and in control. In this context, BRICKSTORM should be viewed as a persistent cyber-espionage instrument of state power, designed to quietly shape the information environment over years rather than days. The true risk it represents is therefore not simply data loss, but the long-term strategic imbalance created when an adversary operates continuously inside the digital nervous system of governments and critical industries.

Seven Strategic Intelligence Insights

While existing adversary reports describe what BRICKSTORM does, the following insights focus on what its behaviour truly signifies at a strategic level. These judgements are derived by correlating activity across multiple investigations and timeframes to surface patterns, intent, and second-order effects that are not explicit in any single report. Together, they reveal how BRICKSTORM functions as a long-term infrastructure access program, not merely a malware campaign.

1) **BRICKSTORM Is a Control-Plane Weapon, Not a Host-Level Backdoor:** BRICKSTORM is consistently positioned within virtualisation platforms, network appliances, and identity control systems, giving it authority over entire environments. This elevates it from a traditional espionage implant to a system-governing access mechanism with enterprise-wide reach.

2) **Its Extreme Dwell Time Is a Design Feature, Not an Outcome:** The ~393-day dwell time reflects intentional engineering choices—delayed execution, cloud-fronted communications, and minimal telemetry generation—explicitly designed to outlast log retention, audits, and incident review cycles.

3) **Identity Control Is the True Strategic Objective:** While email and data access are visible outcomes, the deeper pattern shows systematic abuse of federation services, authentication tokens, secret vaults, and trust relationships. BRICKSTORM is fundamentally about controlling who can become anyone inside a compromised enterprise.

4) **BRICKSTORM Acts as a Strategic Exploit-Development Harvester:** Access to code repositories, development environments, and offline extracted credentials indicates a dual-use mission: operational espionage today and capability building for future cyber operations.

5) **The Campaign Follows a Structured Supply-Chain Access Model:** Repeated compromise of IT and managed service providers before downstream victims reveals a deliberate access-brokerage strategy, where one privileged foothold is used to scale access across multiple organisations.

6) **Appliance Targeting Exploits a Permanent Organisational Blind Spot:** Network appliances and control-plane systems remain poorly inventoried, weakly logged, and rarely hunted in most enterprises. BRICKSTORM is optimised for this structural monitoring failure, not just technical evasion.

7) **The Actor Demonstrates Live Defensive Counter-Intelligence:** Evidence of BRICKSTORM being re-deployed after incident response began confirms the operator’s ability to observe, adapt, and counter defender actions in real time, elevating the threat from static persistence to active defensive contestation.

Recommendations

BRICKSTORM demonstrates that enterprise control planes, not endpoints, are now the primary battleground. Organisations should urgently prioritise the following actions:

1. ***Secure the Control Plane First:*** *Treat virtualisation platforms, identity systems, network appliances, and cloud management layers as Tier-0 assets. These must receive the highest level of hardening, monitoring, and change control.*
2. ***Extend Visibility Beyond EDR and Default SIEM:*** *Instrument hypervisors, identity services, appliances, and management networks with independent telemetry. Assume that endpoint-only coverage is no longer sufficient.*
3. ***Lock Down Privileged Identity at the Infrastructure Layer:*** *Enforce MFA everywhere, eliminate standing admin access, deploy privileged access management, and tightly control service and federation accounts.*
4. ***Restrict Internet Egress from Infrastructure Systems:*** *Hypervisors, management platforms, and identity services should not have unrestricted outbound internet access. Apply explicit allow-listing and continuous egress monitoring.*
5. ***Continuously Validate Security Control Health:*** *Actively monitor for logging gaps, disabled telemetry, and blind spots across non-traditional systems. Missing logs should be treated as a security incident.*
6. ***Harden the Supply Chain and IT Provider Access Model:*** *Assume that trusted providers are potential entry points. Enforce zero-trust access, least privilege, and continuous monitoring of all third-party administrative connections and application updates.*
7. ***Adopt an Assume-Compromise Posture for Tier-0 Systems:*** *Implement proactive threat hunting, integrity monitoring, and continuous baselining for infrastructure and identity platforms, not just reactive alerting.*

BRICKSTORM confirms a decisive shift in modern cyber-espionage: if an adversary controls the control plane, they control the enterprise. Defending against this class of threat requires moving beyond endpoint-centric security toward a control-plane security strategy built on prevention, independent visibility, and continuous verification.

References

Indicator of Compromise Scanner

- https://www.cisa.gov/sites/default/files/2025-12/MAR-251165.c1.v1.CLEAR_stix2.json

BRICKSTORM Indicator of Compromise Scanner

- https://github.com/mandiant/brickstorm-scanner?tab=readme-ov-file

External Intelligence

- https://media.defense.gov/2025/Dec/04/2003834878/-1/-1/0/MALWARE-ANALYSIS-REPORT-BRICKSTORM-BACKDOOR.PDF
- https://blog.nviso.eu/wp-content/uploads/2025/04/NVISO-BRICKSTORM-Report.pdf
- https://www.crowdstrike.com/en-us/blog/warp-panda-cloud-threats/
- https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign