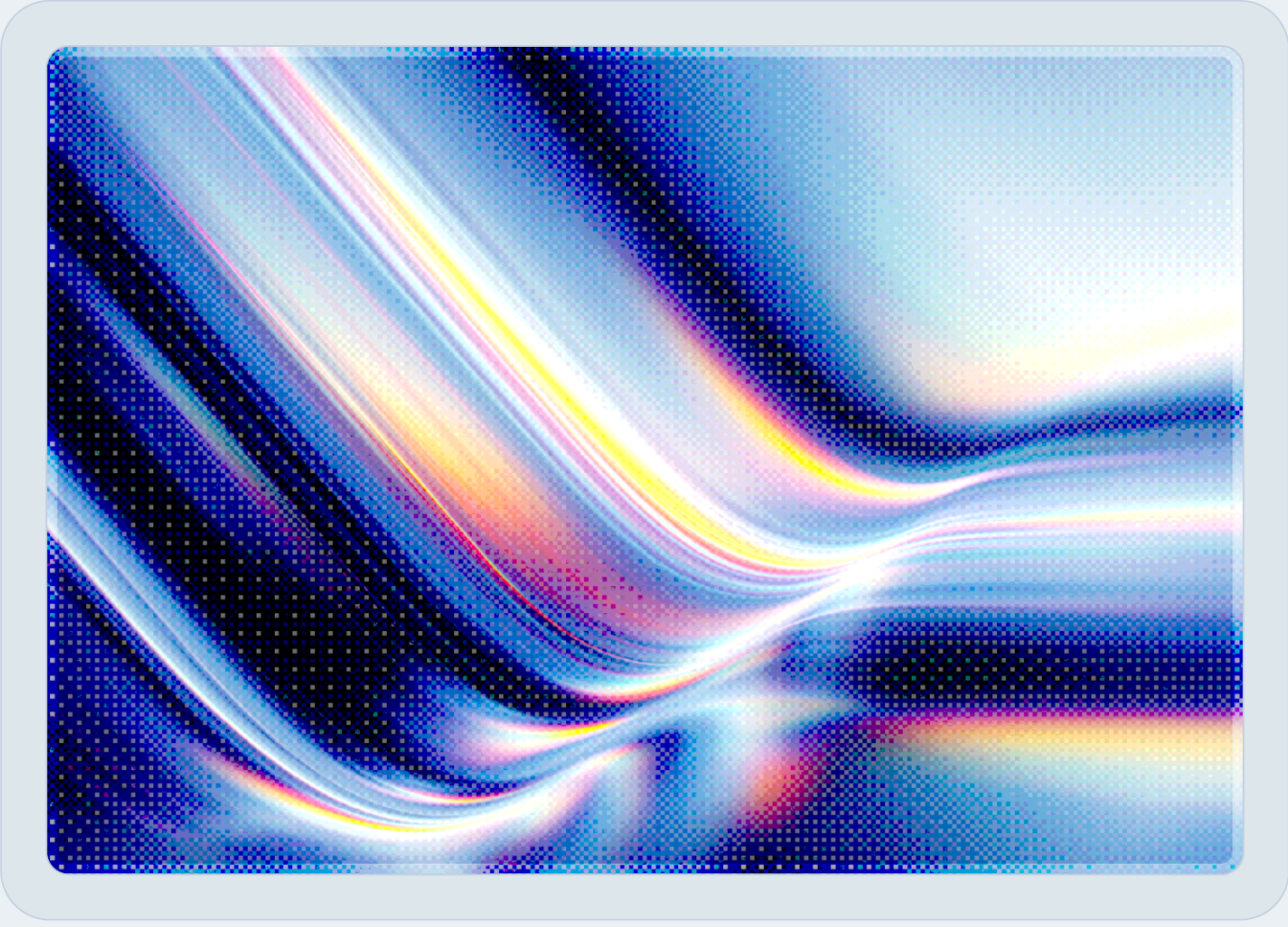
CSAI Foundation | Cloud Security Alliance

VerdantBamboo Deploys BRICKSTORM BSD Variant on Linux Appliances

A China-Nexus APT Compromises Managed Service Providers and Enterprise Storage Systems

2026-06-08

AI-assisted Rapid Research



CSAI | CSA cloud security alliance®

Key Takeaways

- On June 4, 2026, Volexity published findings documenting VerdantBamboo—a China-nexus espionage group tracked by Microsoft as Clay Typhoon, by Google as UNC5221, and by CrowdStrike as Warp Panda—deploying a FreeBSD variant of the BRICKSTORM backdoor and two additional malware families against enterprise Linux storage and network appliances [1] [6].
- VerdantBamboo maintained undetected access to the victim organization for at least 18 months before discovery in September 2025, compromising the victim's Managed Service Provider (MSP) as a lateral access vector and using the MSP's pfSense firewall as a stepping stone [1].
- Three malware families comprise the disclosed toolkit: BRICKSTORM, a Golang/Rust remote access backdoor; PLENET (also tracked as GRIMBOLT by Google), a cross-platform .NET Core backdoor compiled with Native AOT; and AGENTPSD, a Python-based fallback reverse shell [1][2].
- Initial access to the Egnyte Storage Sync appliance was enabled by a local privilege escalation flaw—a misconfigured sudo rule that permitted the unprivileged `egnyteservice` account to write arbitrary files as root—patched in Storage Sync v13.13 (March 2026), with CVE assignment pending [1][5].
- Across all documented BRICKSTORM investigations, the average undetected dwell time is 393 days, a duration that routinely exceeds many organizations' log retention windows and makes retrospective forensics impractical [2].
- Organizations should immediately audit Linux and BSD appliances for BRICKSTORM indicators, enforce multi-factor authentication on all administrative access including MSP-managed accounts, and extend centralized logging and EDR coverage to network-edge appliances that are commonly excluded from standard detection tooling.

Background

VerdantBamboo is a well-resourced cyber espionage actor assessed with high confidence to operate in support of Chinese state intelligence objectives. The group has been active since at least 2023 and is characterized by its preference for targeting network-edge appliances—firewalls, VPN concentrators, NAS devices, and enterprise storage synchronization systems—over endpoints where commercial endpoint detection tools are most densely deployed. This appliance-centric approach is not incidental; VerdantBamboo demonstrates detailed knowledge of proprietary appliance configurations and consistently targets systems that fall outside standard security monitoring programs—a pattern consistent with deliberate evasion of endpoint detection tooling [1][2].

Google's Threat Intelligence Group (GTIG) first publicly associated UNC5221 with BRICKSTORM activity in September 2025, documenting intrusions across legal firms, software-as-a-service providers, business process outsourcers, and technology companies [2]. CISA subsequently issued an advisory in December 2025 confirming PRC state-sponsored actors' use of BRICKSTORM against public sector and information technology targets [3][4]. The Volexity report published June 4, 2026 extends this picture with a detailed incident response case study revealing that the same tooling was adapted for FreeBSD environments and that the threat actor had expanded its persistence mechanism repertoire to include two previously undocumented malware families [1].

The case documented by Volexity illustrates the compounding risk of MSP-dependent infrastructure. The victim organization initially detected suspicious network traffic in September 2025, initiating an incident response engagement. Within days of partial remediation, VerdantBamboo reestablished access —not by re-exploiting the original entry point, but by pivoting through the victim's MSP, specifically through the MSP's pfSense firewall onto which the BSD BRICKSTORM variant had been installed [1]. This sequence demonstrates that remediating the initial victim environment without simultaneously auditing MSP-managed systems may fail to eliminate the threat actor's foothold entirely.

Security Analysis

Attack Chain Reconstruction

The documented intrusion unfolded across at least three distinct phases. In the first phase, VerdantBamboo gained initial access to an Egnyte Storage Sync appliance using valid SSH credentials for the `egnyteservice` account, which is the low-privilege service account used by the application [1]. To elevate privileges, the threat actor exploited a misconfigured sudo rule that allowed the account to

execute the system utility `/usr/bin/tee` as root. Because `tee` writes to files passed as arguments, this misconfiguration effectively granted the ability to write arbitrary content to any location on the filesystem—including protected system directories. This enabled deployment of BRICKSTORM to `/usr/sbin/`, a path that would normally require root permissions [1]. Volexity reported the flaw to Egnyte; a fix was shipped in Storage Sync v13.13 (March 2026) [5], and a CVE identifier is pending assignment.

In the second phase, VerdantBamboo expanded access laterally using stolen administrative credentials. The victim lacked MFA enforcement on MSP-managed accounts, allowing the threat actor to authenticate to the victim organization's firewall and eventually to Microsoft 365 resources through a proxy chain established by the BRICKSTORM SOCKS5 tunneling capability. This credential-based lateral movement bypassed Conditional Access policies [1].

The third phase involved the MSP pivot. Volexity determined that VerdantBamboo had separately compromised the MSP's pfSense firewall, deploying a FreeBSD-compiled variant of BRICKSTORM on that device. This gave the threat actor an independent persistence path that survived the victim organization's own remediation efforts [1]. The MSP pivot also extended the threat actor's reach: any other clients served by the same MSP's firewall infrastructure would be potential targets for further lateral movement.

Malware Families: Technical Profile

Malware	Language	Platform	Capabilities	C2 Protocol
BRICKSTORM (Linux)	Golang / Rust	Linux ELF	Remote shell, SOCKS5 proxy, filesystem web server	WebSocket
BRICKSTORM (FreeBSD)	Golang (gobfuscate-protected)	FreeBSD	Same as Linux variant; obfuscated binary	WebSocket
PLENET / GRIMBOLT	.NET Core (Native AOT)	Cross-platform Linux	Interactive shell, file manipulation, C2 switching	WebSocket + Nerdbank.Streams

Malware	Language	Platform	Capabilities	C2 Protocol
AGENTPSD	Python (PyInstaller)	Linux	Reverse shell (fallback access)	HTTPS POST

BRICKSTORM functions as the primary persistence implant in documented VerdantBamboo operations. Written predominantly in Golang—with some variants subsequently observed in Rust—the backdoor exposes remote command execution, a SOCKS5 proxy server for traffic tunneling, and a filesystem information web server [1][2][4]. Its use of the WebSocket protocol for C2 communications allows traffic to blend with ordinary HTTPS flows, complicating network detection. The FreeBSD variant identified by Volexity was additionally protected with the `gobfuscate` binary obfuscator, which modifies function and variable names to defeat signature-based static analysis [1].

PLENET, which Google Cloud tracks as GRIMBOLT, extends VerdantBamboo's toolkit with a cross-platform implant that operates independently of any .NET runtime, complicating removal and detection. Compiled as a .NET Core application using the Native AOT framework introduced in .NET 7, PLENET produces self-contained native binaries that do not require a .NET runtime installation on the target host [1]. The implant supports interactive shell access, remote command execution, arbitrary file manipulation, and the ability to switch its C2 server on command—the last feature providing resilience against sinkholing or infrastructure takedowns. PLENET uses the Nerdbank.Streams multiplexing library over WebSocket for C2 communications, architecturally similar to BRICKSTORM but independently implemented [1]. Samples observed by Volexity were UPX-compressed.

AGENTPSD functions as a fallback mechanism rather than a primary capability. Written in Python and compiled into a standalone binary using PyInstaller, it implements a basic reverse shell that beacons to a C2 server over HTTPS POST requests [1]. Volexity assessed with high confidence that AGENTPSD was deployed specifically to ensure continued access should the primary BRICKSTORM implant be removed, and it was configured to communicate with a different C2 domain than BRICKSTORM, providing independence across the kill chain.

Infrastructure and Detection Evasion

Across its broader operations documented by Google and Mandiant, VerdantBamboo—operating as UNC5221—demonstrates consistent operational security practices across victim environments. The group uses commercial VPN services including PIA, NordVPN, Surfshark, and VPN Unlimited as egress obfuscation, as well as purpose-built proxy networks constructed from compromised small office and home office (SOHO) routers [2]. The group does not reuse C2 domains across victims, which limits the value of network-based indicators once published [2]. In the September 2025 incident, C2 servers went

dark between September 18 and 23—precisely in the days following the initial IR engagement—before VerdantBamboo reestablished access through the MSP path [1]. The C2 infrastructure was then disabled entirely after Google's public BRICKSTORM report on September 24, 2025, suggesting that the group monitors the threat intelligence community for disclosure events and responds by retiring exposed infrastructure [1].

The average dwell time of 393 days documented across BRICKSTORM investigations [2] routinely exceeds the log retention windows available at many organizations. Many organizations—particularly those outside strictly regulated sectors—maintain log retention windows of 90 to 180 days, placing an intrusion of this duration well outside recoverable log history and making full retrospective reconstruction impractical or incomplete in most enterprise environments. In the documented case, both BRICKSTORM and AGENTPSD had been present on the Storage Sync appliance for at least 18 months before detection, placing their installation well outside any viable forensic lookback window [1].

Scope of Compromise

The systems known to have been compromised or targeted in the documented incident span multiple device categories, illustrating the breadth of the threat actor's access:

System	Role	Status
Egnyte Storage Sync	Enterprise file storage/sync appliance	Confirmed compromised; BRICKSTORM + AGENTPSD deployed
MSP pfSense firewall	FreeBSD-based network firewall	Confirmed compromised; BSD BRICKSTORM deployed
Synology NAS	Network attached storage	Confirmed compromised
VMware vCenter / ESXi	Virtualization infrastructure	Credentials validated; no malware deployed
Microsoft 365	Cloud productivity suite	Accessed via credential theft and proxy chain
GroupWise email server	Legacy email archive	Accessed during lateral movement

The victim organization's Microsoft 365 environment was reached through the BRICKSTORM SOCKS5 proxy, which routed traffic to bypass Conditional Access policies enforced on direct connections [1]. This pattern—using an on-premise or MSP-hosted compromised appliance as a trusted proxy into cloud services—is consistent with UNC5221's broader observed methodology of leveraging internal network positions to circumvent cloud security controls [2].

Recommendations

Immediate Actions

Organizations should treat VerdantBamboo's disclosed tooling as an active threat warranting urgent defensive action, particularly those in the legal, technology, SaaS, and BPO sectors that have been identified as targeting priorities. Any organization using Egnyte Storage Sync should verify that the deployment has been updated to version 13.13 or later, which contains the fix for the privilege escalation flaw exploited in this campaign [1][5]. Organizations should download and run the BRICKSTORM scanner published by Mandiant on GitHub against all Linux and BSD-based appliances in the environment; the tool replicates the primary BRICKSTORM YARA detection logic without requiring a YARA runtime on the target device [7].

For appliances where a scanner cannot be directly executed, reviewing `/usr/sbin/` and other system binary directories for unexpected ELF or statically-linked executables of unusual size is a practical first step. BRICKSTORM Linux samples have been observed at approximately 5.6 MB [1], which is atypically large for a legitimate system utility and may surface in a directory listing review.

Short-Term Mitigations

Multi-factor authentication gaps were a critical structural enabler of VerdantBamboo's lateral movement, demonstrated directly by the threat actor's ability to reestablish access using only stolen credentials after partial remediation. Administrative credentials for MSP-managed systems, firewall management interfaces, VMware vCenter and ESXi, and cloud identity platforms must be protected by MFA without exception. The documented case demonstrates that stolen credentials alone—without any zero-day exploitation—were sufficient for the threat actor to reestablish access and pivot through an MSP to a previously remediated victim [1].

Organizations should audit MSP-granted administrative access with the same rigor applied to internal privileged accounts. This includes reviewing which MSP accounts have access to which devices, whether those accounts are subject to MFA requirements enforced by the organization rather than assumed from the MSP, and whether MSP network connections are logged and monitored. Where feasible, network segmentation should limit MSP management traffic to dedicated, monitored paths rather than general firewall interfaces.

Extending centralized logging to all network-edge appliances—including firewalls, NAS devices, storage sync systems, and VPN concentrators—is essential for reducing dwell time. The 18-month undetected presence in the documented case was facilitated in part by the absence of consistent log collection from the affected appliances [1]. Logs from these devices should be forwarded to a centralized SIEM with sufficient retention to support a meaningful forensic lookback period.

Strategic Considerations

The MSP compromise vector used in this campaign reflects a broader pattern in which supply chain access is leveraged to reach otherwise well-defended organizations. Security teams should formalize MSP risk assessments as part of their vendor management programs, requiring evidence of MFA enforcement, network segmentation, and incident response capabilities from MSPs with privileged access to production infrastructure.

The sustained 393-day average dwell time documented across BRICKSTORM campaigns argues for hunting as a standing practice rather than a reactive activity [2]. Scheduled threat hunts targeting appliance-resident persistence mechanisms—unexpected binaries in system directories, anomalous cron job entries, listening services on non-standard ports—should be conducted on a recurring basis, with frequency calibrated to each organization's risk exposure and the sectors VerdantBamboo has actively targeted. Google's ten-step hunting checklist, published in the September 2025 BRICKSTORM report, provides a structured starting point covering binary scanning, edge device traffic analysis, M365 mailbox access via Enterprise Applications, and VMware VM cloning events [2].

Finally, the use of Native AOT compilation for PLENET signals a deliberate effort to produce implants that function without runtime dependencies and are more resistant to static analysis than interpreted or JIT-compiled code. Security teams should anticipate that detection tooling built around .NET runtime artifacts or managed code signatures will not reliably detect Native AOT-compiled malware, and should test detection coverage against compiled native binaries rather than assuming parity with traditional .NET detection.

CSA Resource Alignment

This campaign is directly relevant to several Cloud Security Alliance frameworks and guidance documents. The MAESTRO threat modeling framework's Layer 1 (Infrastructure and Compute) addresses persistent compromise of appliance and edge infrastructure, and its supply chain threat taxonomy applies to the MSP pivot documented here. Organizations applying MAESTRO to their infrastructure should explicitly scope edge appliances and MSP-managed network devices within their threat models rather than treating them as out-of-scope perimeter devices.

The CSA Cloud Controls Matrix (CCM) addresses relevant controls across multiple domains: Supply Chain Management (STA) for MSP risk oversight, Identity and Access Management (IAM) for the MFA gaps exploited in this campaign, and Logging and Monitoring (LOG) for the centralized log collection requirements that would have materially reduced VerdantBamboo's dwell time. The AI Controls Matrix (AICM), as a superset of CCM, extends these controls to AI-integrated infrastructure and is relevant for organizations where compromised storage or cloud environments intersect with AI training pipelines or model serving infrastructure.

CSA's Zero Trust guidance is applicable to the credential-based lateral movement observed in this campaign. The documented bypass of Microsoft 365 Conditional Access policies through a compromised on-premise proxy illustrates a known Zero Trust enforcement gap: cloud identity policies that evaluate source IP or device compliance do not account for traffic routed through an internally trusted, compromised appliance. Organizations implementing Zero Trust architectures should verify that cloud access policies cannot be circumvented by traffic originating from MSP-managed or appliance-sourced network addresses.

The CSA STAR program and its associated attestation level requirements are relevant for MSP vendor management. Requiring MSPs with privileged network access to maintain STAR Level 2 attestation (or equivalent SOC 2 Type II certification) provides one structured mechanism for establishing a baseline security posture at supply chain partners, though organizations should additionally verify that MSP contracts explicitly require MFA on all privileged accounts and that management access paths are subject to the organization's own monitoring—controls that certification programs may not fully scope.

References

[1] Volexity. "VerdantBamboo: Just Another BRICKSTORM in the Firewall." Volexity Blog, June 4, 2026.

[2] Google Threat Intelligence Group / Mandiant. "Another BRICKSTORM: Stealthy Backdoor Enabling Espionage into Tech and Legal Sectors." Google Cloud Blog, September 24, 2025.

[3] CISA. "PRC State-Sponsored Actors Use BRICKSTORM Malware Across Public Sector and Information Technology Systems." CISA Alert, December 4, 2025.

[4] CISA / Department of Defense. "Malware Analysis Report: BRICKSTORM Backdoor." Joint Malware Analysis Report AR25-338A, December 4, 2025.

[5] Egnyte. "Storage Sync V 13.13 – Miscellaneous Improvements." Egnyte Help Center, March 2026.

[6] The Hacker News. "VerdantBamboo Deploys BSD Variant of BRICKSTORM on Linux Appliances." The Hacker News, June 2026.

[7] Mandiant. "brickstorm-scanner." GitHub, September 2025.