

Forum:[Hack Forums](#)

Thread: [PRC State-Sponsored Actors Use BRICKSTORM Malware Across Public Sector and Informati](#)

Stanley - December 14, 2025, 2:55 am

PRC State-Sponsored Actors Use BRICKSTORM Malware Across Public Sector and Informati

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of ongoing intrusions by People's Republic of China (PRC) state-sponsored cyber actors using BRICKSTORM malware for long-term persistence on victim systems. BRICKSTORM is a sophisticated backdoor for VMware vSphere^{1,2} and Windows environments.³ Victim organizations are primarily in the Government Services and Facilities and Information Technology Sectors. BRICKSTORM enables cyber threat actors to maintain stealthy access and provides capabilities for initiation, persistence, and secure command and control. The malware employs advanced functionality, including multiple layers of encryption (e.g., HTTPS, WebSockets, and nested TLS), DNS-over-HTTPS (DoH) to conceal communications, and a SOCKS proxy to facilitate lateral movement and tunneling within victim networks. BRICKSTORM also incorporates long-term persistence mechanisms, such as a self-monitoring function that automatically reinstalls or restarts the malware if disrupted, ensuring its continued operation.

The initial access vector varies. In one confirmed compromise, PRC state-sponsored cyber actors accessed a web server inside the organization's demilitarized zone (DMZ), moved laterally to an internal VMware vCenter server, then implanted BRICKSTORM malware. See CISA, the National Security Agency, and Canadian Cyber Security Centre's (Cyber Centre's) joint Malware Analysis Report (MAR) BRICKSTORM Backdoor for analysis of the BRICKSTORM sample CISA obtained during an incident response engagement for this victim. The MAR also discusses seven additional BRICKSTORM samples, which exhibit variations in functionality and capabilities, further highlighting the complexity and adaptability of this malware.

After obtaining access to victim systems, PRC state-sponsored cyber actors obtain and use legitimate credentials by performing system backups or capturing Active Directory database information to exfiltrate sensitive information. Cyber actors then target VMware vSphere platforms to steal cloned virtual machine (VM) snapshots for credential extraction and create hidden rogue VMs to evade detection.

CISA recommends that network defenders hunt for existing intrusions and mitigate further compromise by taking the following actions:

- Scan for BRICKSTORM using CISA-created YARA and Sigma rules; see joint MAR BRICKSTORM Backdoor.

- Block unauthorized DNS-over-HTTPS (DoH) providers and external DoH network traffic to reduce unmonitored communications.

- Take inventory of all network edge devices and monitor for any suspicious network connectivity originating from these devices.

- Ensure proper network segmentation that restricts network traffic from the DMZ to the internal network.

See joint MAR BRICKSTORM Backdoor for additional detection resources. If BRICKSTORM, similar malware, or potentially related activity is detected, report the incident to CISA's 24/7 Operations Center at contact@cisa.dhs.gov or (888) 282-0870.

Disclaimer: The information in this report is being provided "as is" for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any

entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

Notes

- 1 Matt Lin et al., "Cutting Edge, Part 4: Ivanti Connect Secure VPN Post-Exploitation Lateral Movement Case Studies," Google Cloud Blog, April 4, 2024, <https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement>.
- 2 Maxime, "NVISO analyzes BRICKSTORM espionage backdoor," NVISO, April 15, 2025, <https://www.nviso.eu/blog/nviso-analyzes-brickstorm-espionage-backdoor>.
- 3 Sarah Yoder et al., "Another BRICKSTORM: Stealthy Backdoor Enabling Espionage into Tech and Legal Sectors," Google Cloud Blog, September 24, 2025, <https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign>.

<https://www.cisa.gov/news-events/alerts/2025/12/04/prc-state-sponsored-actors-use-brickstorm-malware-across-public-sector-and-information-technology>