Lowenstein Sandler

Client Alert

Data Privacy, Security, Safety & Risk Management

December 15, 2025

BRICKSTORM Malware Campaign UPDATE: What Else You Need To Know

By Amy S. Mushahwar and P. Kai Knight

In September 2025, we issued a client alert warning about the BRICKSTORM malware campaign and recommended steps to strengthen your organization's defenses. On Dec. 4, 2025, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency, and Canadian Centre for Cyber Security released a report, Malware Analysis Report AR25-338A (BRICKSTORM Backdoor), which confirms our initial assessment and provides expanded technical details, detection signatures, and mitigation guidance.

The report concludes that People's Republic of China state-sponsored actors are deploying BRICKSTORM to achieve long-term persistence in VMware vSphere (vCenter/ESXi) and Windows environments. The primary targets appear to be government services and facilities, along with information technology companies supporting this sector. If you operate in these areas, remain vigilant and review the details below carefully. Please note, this is a very stealthy attack and without proactive triage and indicator of compromise scanning, these compromises will remain invisible, and organizations will not know they've been breached.

Updated Information About How BRICKSTORM Works

The report is based on data CISA collected from eight BRICKSTORM samples originating from affected organizations; each sample provided threat actors with access as well as capabilities for initiation, persistence, and secure command and control operations.

According to the report, after being launched, BRICKSTORM performs checks and can reinstall and restart itself to stay persistent. To function properly, it sets up environmental variables that are tailored to the compromised system. Its persistence relies on a self-monitoring feature that reinstalls and restarts BRICKSTORM if it detects that the process isn't working as intended. Once initial checks are successful, BRICKSTORM connects securely to a command-and-control server, giving the threat actor full access to the compromised system–including file system management, interactive shell commands usage, and the ability to move laterally within the network. For additional technical details on the malware functionality and delivery, please refer to the CISA report.

The Report's Conclusions

Most important, the report includes indicators of compromise and detection tools, which were unavailable for our September alert. CISA recommends deploying CISA-created YARA rules to detect malicious activity and provides guidance on how to identify activity with those rules. CISA also recommends using a CISA-created Sigma rule to detect BRICKSTORM. Finally, the report provides mitigations that will improve cybersecurity posture, and we provide a brief summary of these at the end of this alert for your convenience.

Why Government Contractors Should Act Now

Chinese state-sponsored threat actors are known for stealth and persistence. They rarely seek immediate disruption; instead, they aim for long-term access to sensitive systems and data. BRICKSTORM exemplifies this approach in the following ways:

- Stealth techniques: Encrypted communications, DNS-over-HTTPS (DoH) traffic, and virtualization-aware features make detection difficult.
- Trusted environment exploitation: By targeting VMware vSphere and service accounts, attackers blend into legitimate operations.
- Supply chain risk: Contractors often provide indirect access to government networks, making them prime targets for espionage and intellectual property theft.

Strategic takeaway: Assume compromise is possible. Focus on detection and containment, not just prevention. Continuous monitoring, threat hunting, and strict access controls are essential to counter these advanced tactics.

Why This Matters

This update reinforces the urgency of implementing the mitigations outlined in our original alert and adopting CISA's new detection tools. Organizations in the targeted sectors should act immediately to reduce exposure and strengthen defenses.

For full technical details, see the official CISA report:

Recommended Mitigation Measures

For this attack pattern, the recommended mitigations include:

- Upgrade VMware vSphere servers to the latest version.
- Harden your VMware vSphere environments by applying VMware's guidance.
- Take inventory of all network edge devices and monitor for any suspicious network connectivity originating from these devices.
- Ensure proper network segmentation restricts network traffic from the DMZ to the internal network.
- Disable Remote Desktop Protocol and Server Message Block from the demilitarized zone network to the internal network.
- Apply the principle of least privilege and restrict service accounts to only needed permissions.
- Increase monitoring for service accounts, which are highly privileged and have a predictable pattern of behavior (e.g., scans that reliably run at a certain hour of the day).
- Block unauthorized DoH providers and external DoH network traffic to reduce unmonitored communications.

Act now to implement these mitigations and deploy detection tools. Contact Amy S. Mushahwar, P. Kai Knight, or the Lowenstein lawyer with whom you normally work for further assistance. Stay vigilant, and we especially encourage action for government contractors and the IT services organizations that serve them.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data Privacy, Security, Safety & Risk Management
T: 202.753.3825
amushahwar@lowenstein.com

P. KAI KNIGHT
Counsel
T: 202.753.3828
kknight@lowenstein.com

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.