

Forum:[Hack Forums](#)

Thread: [CISA and Partners Release Update to Malware Analysis Report BRICKSTORM Backdoor](#)

Stanley - January 19, 2026, 2:55 pm

CISA and Partners Release Update to Malware Analysis Report BRICKSTORM Backdoor

Today, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency, and Canadian Centre for Cyber Security released an update to the Malware Analysis Report BRICKSTORM Backdoor with indicators of compromise (IOCs) and detection signatures for additional BRICKSTORM samples. This update provides information on additional samples, including Rust-based samples. These samples demonstrate advanced persistence and defense evasion mechanisms, such as running as background services, and enhanced command and control capabilities through encrypted WebSocket connections.

The update includes two new detection signatures in the form of YARA rules, enabling organizations to better identify BRICKSTORM-related activity. Organizations are strongly encouraged to deploy these updated IOCs and signatures, and to follow the detection guidance to scan for and respond to BRICKSTORM infections. 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.

<https://www.cisa.gov/news-events/alerts/2025/12/19/cisa-and-partners-release-update-malware-analysis-report-brickstorm-backdoor>