CTI Evaluation Report

BRICKSTORM Backdoor

Field	Value
Conversion type	STIX 2.1 → MISP
Conversion date	2025-12-13 08:48
Report generated	2026-07-08 14:31 UTC
UUID	`b1c44881-e2d6-46c4-b39a-3613ed20eb67`
Visibility	Public

> The Cybersecurity and Infrastructure Security Agency (CISA) analyzed eight BRICKSTORM samples obtained from victim organizations. BRICKSTORM is a custom Executable and Linkable Format (ELF) Go-based backdoor. The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Canadian Centre for Cyber Security (Cyber Centre) assess People's Republic of China (PRC) state-sponsored cyber actors are using BRICKSTORM malware for long-term persistence on victim systems.

BRICKSTORM enables cyber actors to maintain stealthy access and provide capabilities for initiation, persistence, and secure command and control (C2). BRICKSTORM initiates by running checks and maintains persistence by using a self-watching function and automatically reinstalls or restarts if disrupted.

For C2, BRICKSTORM uses multiple layers of encryption (HTTPS, WebSockets, nested Transport Layer Security [TLS]) to hide its communications with the cyber actors' C2 server. It also uses DNS-over-HTTPS (DoH) and mimics web server functionality to blend its communications with legitimate traffic. For remote system control, BRICKSTORM gives cyber actors interactive shell access on the system and allows them to browse, upload, download, create, delete, and manipulate files. Some samples act as a SOCKS proxy, facilitating lateral movement and allowing cyber actors to compromise additional systems, and some samples use a virtual socket (VSOCK) interface to enable inter-virtual machine (VM) communication, support data exfiltration, and maintain persistence in virtualized environments.

Overall Score: ○ No data (N/A)

Community assessment based on **0 vote(s)** from the CTI-Transmute platform.

- **0 like(s)**

Methodology

Scores are derived from community votes on the **CTI-Transmute** platform using the MISP cti-evaluation taxonomy.

Level	Numeric score
very-low	0/100
low	25/100
moderate	50/100
high	75/100
very-high	100/100

The **overall score** is the mean of all dimension votes. The **consensus level** for a dimension requires at least 2 votes on the same level.

Generated by CTI-Transmute — 2026-07-08 14:31 UTC