Chinese Hackers Use ‘BRICKSTORM’ Backdoor to Breach US Firms

Data: 2025-09-25 12:30:00

Autor: Inteligência Against Invaders

The GITG researchers argued that the motivation of these attacks “extends beyond typical espionage missions, potentially providing data to feed development of zero-days and establishing pivot points for broader access to downstream victims.”

In many occurrences, the threat actors were particularly interested in the emails of key individuals within the victim organizations and sometimes exfiltrated files from these emails.

Google has attributed these campaigns to UNC5221, a Chinese-aligned threat cluster linked to sophisticated capabilities, including the exploitation of zero-day vulnerabilities targeting network appliances.

While other security vendors consider UNC5221 and Silk Typhoon to be the same group, GTIG currently tracks them as two distinct entities.

Sophisticated Campaigns Against US Organizations

The Google report noted that the GTIG investigation into the BRICKSTORM campaigns had been made particularly difficult because of the threat actors’ speed in deploying the full attack chain.

“In many cases, the average dwell time of 393 days exceeded log retention periods and the artifacts of the initial intrusion were no longer available,” the researchers wrote.

Nevertheless, they found that UNC5221 used a range of sophisticated techniques to maintain persistence and minimize the visibility traditional security tools have into their activities.

These include:

1. **Initial access:** exploiting zero-day vulnerabilities
2. **Establishing foothold:** BRICKSTORM deployment on appliances that do not support traditional endpoint detection and response (EDR) tools (e.g. VMware vCenter and ESXi hosts)
3. **Escalating privilege:** In-memory Servlet filter injection, credential harvesting via HTTP basic auth, bypassing MFA protections, VM cloning of critical servers, targeting Delinea Secret Server, execution of automated secret stealer tools
4. **Moving laterally:** credential reuse from vaultsand scripts
5. **Establishing persistence:** init.d, rc.local, or systemd file changes to ensure BRICKSTORM starts on appliance reboot
6. **Completing mission:** exploiting Microsoft Entra ID Enterprise Applications with mail.read or full_access_as_app scopes to access the email mailboxes of target accounts

Inside the BRICKSTORM Backdoor

BRICKSTORM Forensics Analysis

BRICKSTORM is a Go backdoor targeting VMware vCenter servers.

According to a previous Google report, published in April 2024, the backdoor supports the ability to set itself up as a web server, perform file system and directory manipulation, perform file operations such as upload/download, run shell commands, and perform SOCKS relaying.

BRICKSTORM communicates over WebSockets to a hard-coded command-and-control(C2) server.

Upon execution, BRICKSTORM checks for an environment variable, WRITE_LOG, to determine if the file needs to be executed as a child process. If the variable returns false or is unset, it will copy the BRICKSTORM sample from /home/vsphere-ui/vcli to /opt/vmware/sbin as vami-httpd. It will then execute the copied BRICKSTORM sample and terminate execution.

If WRITE_LOG is set to true, it assumes it is running as the correct process, deletes /opt/vmware/sbin/vami-httpd, and continues execution.

BRICKSTORM contains a separate function called Watcher, which contains self-monitoring functionality. If the environment variable WORKER returns false or is unset, it will continue the monitoring, checking for the file /home/vsphere-ui/vcli and copying the contents over to /opt/vmware/sbin/vami-httpd. Then, it sets the appropriate environment variables and spawns the process. The watcher process then begins monitoring the exit status of the child process.

If it finds the environment variable WORKER is set to true, it assumes it is a spawned worker process meant to execute the backdoor functionality and skips the remainder of the Watcher function.

BRICKSTORM communicates with the C2 using WebSockets. This sample contains a hard-coded WebSocket address of wss://opra1.oprawh.workers[.]dev. Additionally, it contains the following legitimate DNS over HTTPS (DoH) addresses.

BRICKSTORM Deployment

Typically, threat actors deploy the backdoor to a network appliance before pivoting to VMware systems.

The hackers then move laterally to a vCenter server in the environment using valid credentials, which were likely captured by the malware running on the network appliances.

In April 2025, European cybersecurity company NVISO discovered two new BRICKSTORM samples affecting Windows environments.

These samples had been used to spy on European organizations via Windows since at least 2022, NVISO said.

While Google has acknowledged the NVISO report, it said it has not observed BRISTORM Windows-focused variants in any investigation to date.

Google’s Mandiant has released a scanner script that can run on *nix-based appliances and other systems without requiring YARA to be installed.

The tool is designed to replicate a specific YARA rule (G_APT_Backdoor_BRICKSTORM_3) by searching for a combination of strings and hex patterns unique to the backdoor.