BRICKSTORM Malware: UNC5221 Targets Tech and Legal Sectors in the United States

By Huseyin Can YUCEEL

Published: 2025-09-25 · Archived: 2026-04-29 02:10:20 UTC

State-sponsored threat actors that specialize in cyber espionage operate with silence as their defining trait. Their aim is not disruption but invisibility. They infiltrate systems quietly, establish persistence that blends into normal operations, and exfiltrate valuable data without raising alarms.

BRICKSTORM embodies this approach. First identified in March 2025, the backdoor has been leveraged by the cluster tracked as UNC5221, designed to persist in environments for months at a time while providing operators with stealthy, long-term access. With average dwell times extending nearly a year, BRICKSTORM has successfully exfiltrated data from legal services, SaaS providers, and technology organizations in the United States.

In this blog post, we explain the Tactics, Techniques, and Procedures (TTPs) used by UNC5221 and how organizations can defend themselves against BRICKSTORM malware attacks.

Brickstorm Malware Explained

BRICKSTORM malware is a cross-platform backdoor attributed to the UNC5221 cluster, a China-nexus APT. Written in Go and tailored for appliance and management software environments, the backdoor has variants that run on Linux, Windows, and BSD-based devices. BRICKSTORM provides a SOCKS proxy that lets operators tunnel into internal networks for interactive access and file retrieval, and it accepts web-based commands, executing them on the host and returning output via HTTP responses. Operators routinely modify and obfuscate samples (often using **Garble**) and sometimes embed delayed-start logic so deployed implants remain dormant until after incident responders have left, a tactic that increases the likelihood of long-term, undetected persistence.

UNC5221 mainly targets legal services, Software-as-a-Service providers, business process outsourcers, and technology firms. These verticals provide rich intelligence, access to downstream customers, and intellectual property useful for further exploit development. Initial access is often linked to compromise of perimeter or remote-access appliances. Once on an appliance, the actor leverages BRICKSTORM for persistent remote access and uses the malware's SOCKS proxy to reach internal web applications, code repositories, and file shares directly from their workstation. The operator's lateral movement is typically credential-driven. They harvest or extract credentials from appliances, password vaults, or intercepted web authentication flows and then use those legitimate credentials to access vCenter/ESXi and Windows systems. A recurring and notable operational technique is cloning sensitive virtual machines in vCenter, mounting the clone offline to extract credential stores such as ntds.dit, and then deleting the clone to minimize detection risk.

TTPS Used by BRICKSTORM Malware and the UNC5221 Group

Initial Access

T1190 Exploit Public-Facing Application

BRICKSTORM intrusions frequently begin with the compromise of edge appliances and other public-facing management interfaces. In at least one documented case, the actor exploited a vulnerability in an appliance to gain an initial foothold. Exploiting appliances is a recurring pattern because management-plane devices often lack standard endpoint telemetry and are retained longer than ordinary servers. This makes appliance exploitation an attractive vector for a stealthy operator who wants silent, persistent entry.

Execution

T1059 Command and Scripting Interpreter

Once deployed, BRICKSTORM can accept web-based commands and execute arbitrary OS commands, returning the command output in HTTP responses. The backdoor's ability to run commands via HTTP gives operators interactive control without needing interactive shells that endpoint tools more readily detect, enabling hands-on investigation, data collection, and targeted actions while remaining difficult to observe from standard host telemetry.

Persistence

T1505.003 Server Software Component: Web Shell

In virtual infrastructure, threat actors installed an in-memory Java Servlet filter called BRICKSTEAL into vCenter's Tomcat to intercept and decode web authentication flows and harvest credentials. Since it runs in memory with no obvious new files, the filter can persist across service cycles and provide stealthy, long-lived access to management interfaces.

T1547 Boot or Logon Autostart Execution

UNC5221 establishes persistence by modifying startup scripts or systemd units so the implant survives reboots.

sed -i s/export TEXTDOMAIN=vami-lighttp/export TEXTDOMAIN=vami-lighttp\n\/path/to/brickstorm/g /opt/vmware/etc/init.d/vami-lighttp

sed -i $a\SETCOLOR_WARNING="echo -en `/path/to/brickstorm`\\033[0;33m" /etc/sysconfig/init

Credential Access & Privilege Escalation

T1555 Credentials from Password Stores

UNC5221 operators actively target centralized secret stores and password vaults to harvest high-value credentials. After gaining access to management infrastructure, they move to systems where credentials are aggregated, and they extract or decrypt vault contents to obtain service accounts and privileged credentials. This approach yields broad access while minimizing noisy behaviors on endpoints. Threat actors commonly target the following password stores.

- Browser profile paths: %appdata%\Mozilla\Firefox\Profiles
- Appdata locations used to store session tokens: Users\<username>\.azure\
- Windows credential vault: %appdatalocal%\Microsoft\Credentials
- Data Protection API (DPAPI) keys: %appdata%\Microsoft\Protect\<SID>\

T1003 OS Credential Dumping

UNC5221 has used virtualization management capabilities to clone critical VMs, mount the clones offline, and extract credential stores such as **ntds.dit**. By operating against an offline clone, the actor avoids endpoint controls and behavioral detections that would trigger on the production host, while still obtaining the same high-value authentication artifacts like password hashes and cached credentials. After VM cloning and offline extraction, threat actors attempted to remove forensic traces.

Lateral Movement

T1021.004 Remote Services: SSH

UNC5221 frequently uses SSH to move between appliances and management hosts. After compromising valid accounts, operators connect over SSH from compromised appliances to vCenter, ESXi hosts, and other internal systems to copy files, install tools, and execute commands without spawning obvious interactive shells on endpoints. In several incidents, the actor enabled SSH remotely via vCenter's VAMI interface, created short-lived local accounts to stage payloads or perform configuration changes, and then removed those accounts to reduce forensic artifacts. These actions blend into normal administrative operations and reduce the opportunity for detection in environments where SSH is a legitimate management channel.

Defense Evasion

T1027 Obfuscated Files or Information

BRICKSTORM malware variants are routinely obfuscated and modified for each victim to bypass signature-based detection and static analysis. Operators build Go binaries with obfuscation tooling and strip identifying strings or symbols so that malware appearing on disk does not match known indicators. They also design workflows that minimize disk-resident artifacts like staging or executing components in memory, removing installer files after execution, and hiding functionality inside legitimate management processes. The combination of per-victim binary variations and in-memory techniques makes detection by traditional file-hash or string-based signatures unreliable.

Command and Control

T1071.001 Application Layer Protocol: Web Protocols

BRICKSTORM uses common web protocols to blend command-and-control traffic into routine HTTPS activity, making network-based detection more difficult. The implant periodically issues web requests to third-party platforms and developer hosting services and accepts commands and payloads over HTTP/HTTPS, which allows operators to hide malicious exchanges inside apparently normal encrypted web traffic. The backdoor's SOCKS proxy capability further amplifies this effect by allowing an operator's workstation to route through the compromised appliance and interact directly with internal services, turning the victim into a pivot point for deeper operations while all outward traffic looks like ordinary web connections.

T1071.004 Application Layer Protocol: DNS over HTTPS

As an additional layer of stealth, BRICKSTORM has been observed using DNS over HTTPS (DoH) to resolve command-and-control infrastructure and to obscure DNS activity from traditional DNS inspection. DoH encapsulates DNS queries in HTTPS, which both encrypts resolution traffic and allows it to blend with normal web browsing flows, complicating detection and blocking efforts that rely on plain DNS visibility. Operators combine DoH with shifting, ephemeral infrastructure like Cloudflare Workers, Heroku, and commercial VPN exit nodes so that domain resolution and subsequent C2 connections look like routine encrypted web traffic, further reducing the signal available to defenders.

Exfiltration

T1041 Exfiltration Over C2 Channel

BRICKSTORM operators move stolen data out of victim environments using the same covert channels they use for command and control so that exfiltration traffic blends with otherwise normal encrypted web connections.

BRICKSTORM leverages SOCKS proxy to pivot an operator's workstation into the target network and then pull files directly from internal shares, code repositories, or endpoints through that tunnel. Since the transfer appears to originate from an internal management appliance, it can look like legitimate administrative traffic. Operators also layer additional obfuscation by routing egress through commercial VPN providers or ephemeral third-party platforms to decouple victims from consistent domains and frustrate IP/domain-based blocking.

In parallel, the group has abused Microsoft Entra enterprise-app permissions like mail.read and full_access_as_app to collect mailbox contents at scale, which is a form of high-volume, targeted data extraction that bypasses host-level file transfers entirely.

How Picus Helps Simulate UNC5221 and BRICKSTORM Backdoor Attacks?

We also strongly suggest simulating the **UNC5221 and BRICKSTORM backdoor attacks** to test the effectiveness of your security controls against sophisticated cyber attacks using the **Picus Security Validation**

Platform. You can also test your defenses against other malware attacks, such as XZ Utils backdoor, Androxgh0st, and StealC, within minutes with a 14-day free trial of the Picus Platform.

Picus Threat Library includes the following threats for **UNC5221 and BRICKSTORM backdoor attacks**:

Threat ID	Threat Name	Attack Module
61516	UNC5221 Threat Group Campaign	Linux Endpoint
81651	UNC5221 Threat Group Campaign Malware Download Threat	Network Infiltration
38486	UNC5221 Threat Group Campaign Malware Email Threat	Email Infiltration (Phishing)
95424	BRICKSTORM Backdoor Malware Download Threat	Network Infiltration
85776	BRICKSTORM Backdoor Malware Email Threat	Email Infiltration (Phishing)

Picus also provides actionable mitigation content. **Picus Mitigation Library** includes prevention signatures to address **UNC5221 and BRICKSTORM backdoor** and other ransomware attacks in preventive security controls. Currently, Picus Labs has validated the following signatures for **UNC5221 and BRICKSTORM backdoor**:

Security Control	Signature ID	Signature Name
Check Point NGFW	0B789E2F7	Backdoor.Win32.Tesdat.TC.b847onmJ
Check Point NGFW	0BB84904E	Backdoor.Linux.BrickStorm.TC.4310JXYu
Check Point NGFW	09698A46C	Backdoor.Linux.BrickStorm.TC.201bYxCy
Cisco FirePower		Elf.Rootkit.RESURGE.tii.Talos
Forcepoint NGFW		File_Malware-Blocked

FortiGate AV	10210769	Linux/Agent.AHD!tr
FortiGate NGFW	10232948	ELF/Agent.D041!tr
FortiGate NGFW	10232947	ELF/Agent.1FCC!tr
Palo Alto	710626769	trojan/Linux.apitw.a
Trellix	0x4840c900	MALWARE: Malicious File Detected by GTI

Start simulating emerging threats today and get actionable mitigation insights with a **14-day free trial** of the Picus Security Validation Platform.
