Lowenstein Sandler

Client Alert

Data Privacy, Security, Safety & Risk Management

September 25, 2025

BRICKSTORM Malware Campaign: What You Need To Know

By Amy S. Mushahwar, Carly E. Nixon, and Chloe Rippe

What's Happening:

Recent investigations by leading threat intelligence and incident response teams have identified a sophisticated and persistent cyber campaign leveraging the BRICKSTORM malware, attributed to UNC5221 and related China-linked threat clusters. The campaign has targeted a broad spectrum of U.S. organizations, including legal services, SaaS providers, business process outsourcers, and technology firms. The threat actors demonstrate advanced capabilities in maintaining long-term, stealthy access to victim environments, with a particular focus on appliances and virtualization infrastructure that often lack traditional security controls. We recommend using Mandiant's BRICKSTORM scanner to help combat this threat.

How They Operate:

The BRICKSTORM campaign is characterized by a multi-stage lifecycle, including initial access, establishment of persistence, privilege escalation, lateral movement, and data exfiltration. Key aspects of the threat actors' methodology include:

- Initial Access: The actors frequently compromise perimeter and remote access infrastructure, often exploiting zero-day vulnerabilities in network appliances. Due to the extended dwell time (averaging 393 days), forensic evidence of initial access is often unavailable.
- Persistence: BRICKSTORM, a Go-based backdoor with SOCKS proxy functionality, is deployed on Linux and BSD-based appliances, particularly those not monitored by endpoint detection and response (EDR) tools. The malware is designed to blend in with legitimate processes and is often obfuscated to evade detection.
- Privilege Escalation: The actors have deployed malicious Java Servlet filters (BRICKSTEAL) on VMware vCenter servers to capture credentials, including those with high privileges. They have also cloned virtual machines containing sensitive data, such as domain controllers and credential vaults, without powering them on to avoid triggering security tools.
- Lateral Movement: The actors use valid credentials, often harvested from compromised password vaults or scripts. The actors enable SSH on targeted appliances and use legitimate administrative interfaces to propagate BRICKSTORM.
- Data Exfiltration: The campaign has consistently sought access to and exfiltration of emails of key personnel, source code repositories, and sensitive files. Exfiltration is conducted via the SOCKS proxy feature of BRICKSTORM and through the abuse of Microsoft Entra ID Enterprise Applications with broad mail access permissions.

What You Should Do:

Because of the high operational security and lack of reusable indicators of compromise (IOCs), traditional signature-based detection is largely ineffective against BRICKSTORM. Organizations are advised to adopt a Tactics, Techniques, and Procedures (TTP)-based hunting approach, with the following recommended actions:

- Asset Inventory: Maintain an up-to-date inventory of all appliances and edge devices, including those not covered by standard security tools.
- File and Backup Scanning: Utilize YARA rules and provided scanner scripts to identify BRICKSTORM binaries on appliances and in backup data stores.
- Network Traffic Analysis: Monitor outbound traffic from appliance management interfaces for suspicious connections, particularly to non-vendor domains or use of DNS over HTTP.
- Windows System Access: Investigate network logins and RDP sessions from appliances to Windows servers and desktops and analyze Windows User Access Logs for anomalous activity.
- Credential and Secret Access: Examine Windows Shellbags and other forensic artifacts for unauthorized access to credential stores and sensitive directories.
- M365 Mailbox Access: Audit Microsoft 365 Enterprise Applications for excessive mail access permissions and review mail access logs for anomalous patterns, including the use of commercial VPNs and obfuscation networks.
- VMware Activity: Review vCenter and ESXi logs for evidence of unauthorized VM cloning, local account creation, SSH enablement, and rogue VM deployments.

Hardening and Mitigation Recommendations:

To reduce exposure:

- Restrict internet and internal network access for appliances to only what is necessary for business operations.
- Enforce multi-factor authentication (MFA) for administrative interfaces and critical systems.
- Centralize and retain security logs for extended periods to facilitate forensic investigations.
- Apply strict access controls and isolation to credential vaulting systems, treating them as Tier 0 assets.
- Work with vendors to implement secure software practices, such as hardware-based key storage.

Final Thoughts:

BRICKSTORM reflects a broader trend of targeting appliances and virtualization infrastructure to achieve espionage, intellectual property theft, and enable further exploit development. The targeting of legal, SaaS, and technology sectors underscores the strategic objectives of the threat actors, including access to sensitive national security, trade, and proprietary information. Organizations are strongly encouraged to reassess their threat models, enhance visibility into non-traditional assets, and adopt proactive threat-hunting practices to defend against this evolving threat landscape.

For questions, please contact the authors.

Contacts

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

AMY S. MUSHAHWAR
Partner
Chair, Data, Privacy & Cybersecurity
T: 202.753.3825
amushahwar@lowenstein.com

CARLY E. NIXON
Associate
T: 212.419.5889
cnixon@lowenstein.com

CHLOE RIPPE
Associate
T: 212.419.5895
crippe@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.