Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

BRICKSTORM Malware Quietly Builds the Perfect Hideout in US Networks

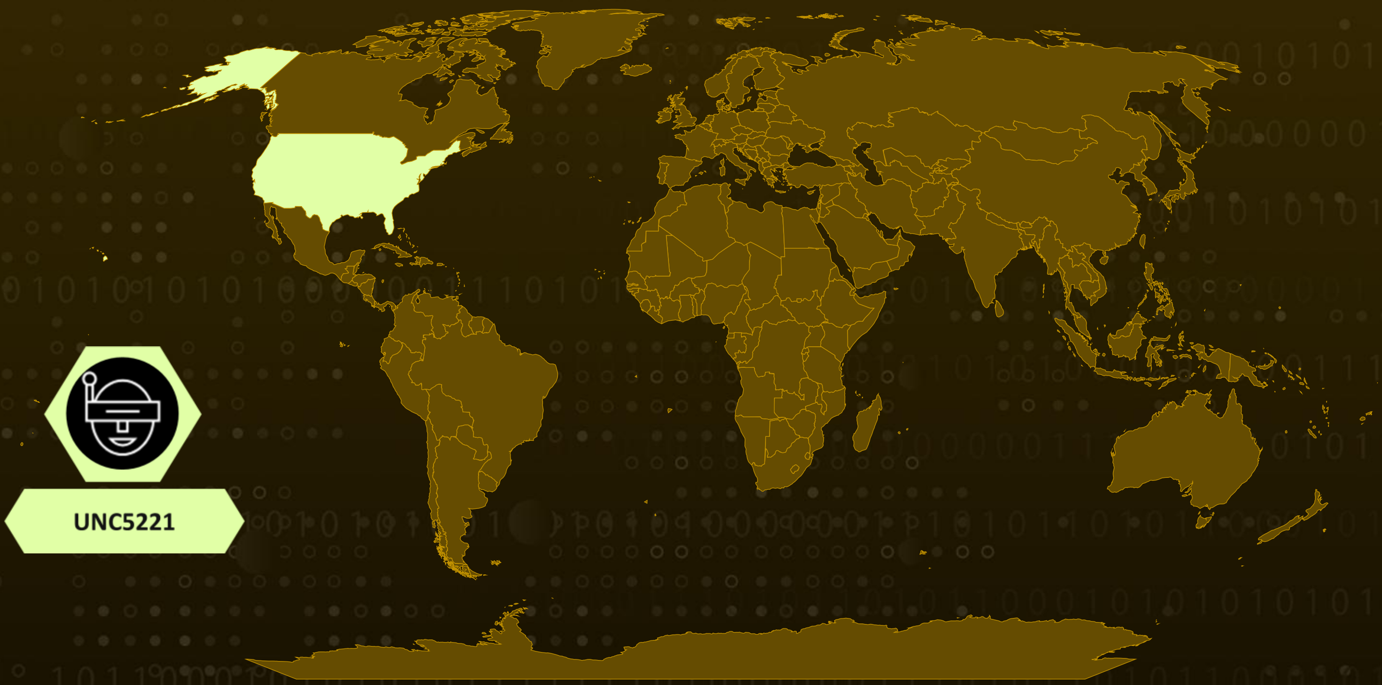
Date of Publication	Admiralty Code	TA Number
September 26, 2025	A1	TA2025299

Summary

Attack Commenced: March 2025
Malware: BRICKSTORM
Threat Actor: UNC5221 (alias UTA0178, Red Dev 61)
Targeted Country: United States
Targeted Industries: Legal, Software-as-a-Service (SaaS) Providers, Business Process Outsourcers (BPOs), Technology

Attack: BRICKSTORM, a Go-based backdoor linked to the China-nexus threat group UNC5221, has been actively targeting U.S. organizations since March 2025 by exploiting Ivanti Connect Secure vulnerabilities and compromising network appliances that lack EDR coverage. Beyond standard espionage, these intrusions capture sensitive information that enables zero-day discovery and creates durable access points for lateral expansion.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Since March 2025, the BRICKSTORM malware has been used to maintain persistent access to organizations in the United States across multiple industries. These operations extend beyond standard espionage, providing data useful for developing zero-day vulnerabilities and creating footholds to reach additional downstream victims.

#2 The China-linked cyber-espionage group UNC5221 is responsible, exploiting network appliances that cannot support traditional endpoint detection and response (EDR) agents to deploy new variants of the BRICKSTORM backdoor. BRICKSTORM, a Go-based backdoor, was first documented in early 2024 during the exploitation of Ivanti Connect Secure vulnerabilities (CVE-2023-46805 and CVE-2024-21887).

#3 In at least one case, these flaws were used to gain initial access and install the malware. However, in many other intrusions, prolonged dwell times and the group's deliberate removal of evidence have obscured the exact infection vectors for Linux and BSD-based appliances.

#4 BRICKSTORM further enhances its ability to evade detection, enabling intrusions to persist undetected for an average of 393 days. Another advanced technique involves cloning sensitive virtual machines (VMs) from VMware vCenter servers, with a focus on domain controllers and password vaults. The campaign deploys a malicious Java Servlet filter for Apache Tomcat, dubbed BRICKSTEAL, to harvest vCenter credentials and achieve privilege escalation.

#5 Overall, BRICKSTORM represents a highly adaptive espionage toolkit that combines stealth, credential theft, VM manipulation, and cloud mailbox exploitation. The ultimate objective is to compromise the communications of high-value individuals, including developers, system administrators, and personnel linked to areas of strategic interest to China's economic and intelligence priorities.

Recommendations

Monitoring Non-EDR Appliances: Enhance monitoring for appliances that cannot support EDR by implementing agentless solutions. Centralize the collection of syslogs, process data, network flows, and configuration snapshots. Supplement this with network IDS/IPS and packet capture capabilities to improve visibility into east-west traffic.

Harden Management Interfaces: Restrict administrative access to management networks, enable role-based access control (RBAC) with least privilege, require jump hosts for console access, and disable unnecessary services.

Implement Network Segmentation and Zero Trust Architecture: Segment networks to limit malware spread across interconnected systems. Apply zero trust principles, verify identity and device posture before granting access, regardless of location. Use micro-segmentation tools to define fine-grained access rules.

Regularly Review and Harden File System Permissions: Audit permissions for sensitive directories and ensure that only essential processes and users have write access. Disable file sharing where not required and use access control lists (ACLs) to limit exposure.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**T1190** Exploit Public-Facing Application
T1078 Valid Accounts	**T1136** Create Account	**T1543** Create or Modify System Process	**T1027** Obfuscated Files or Information

T1021 Remote Services	**T1021.001** Remote Desktop Protocol	**T1555** Credentials from Password Stores	**T1673** Virtual Machine Discovery
T1564 Hide Artifacts	**T1564.006** Run Virtual Instance	**T1114** Email Collection	**T1114.002** Remote Email Collection
T1671 Cloud Application Integration	**T1003** OS Credential Dumping	**T1087** Account Discovery	**T1059** Command and Scripting Interpreter
T1505.003 Web Shell	**T1547** Boot or Logon Autostart Execution	**T1021.004** SSH	**T1071.001** Web Protocols
T1041 Exfiltration Over C2 Channel	**T1071.004** DNS	**T1567** Exfiltration Over Web Service	**T1071** Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035, 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df, aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878

References

https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign

https://hivepro.com/threat-advisory/two-zero-day-flaws-found-in-ivanti-connect-secure-and-policy-secure/

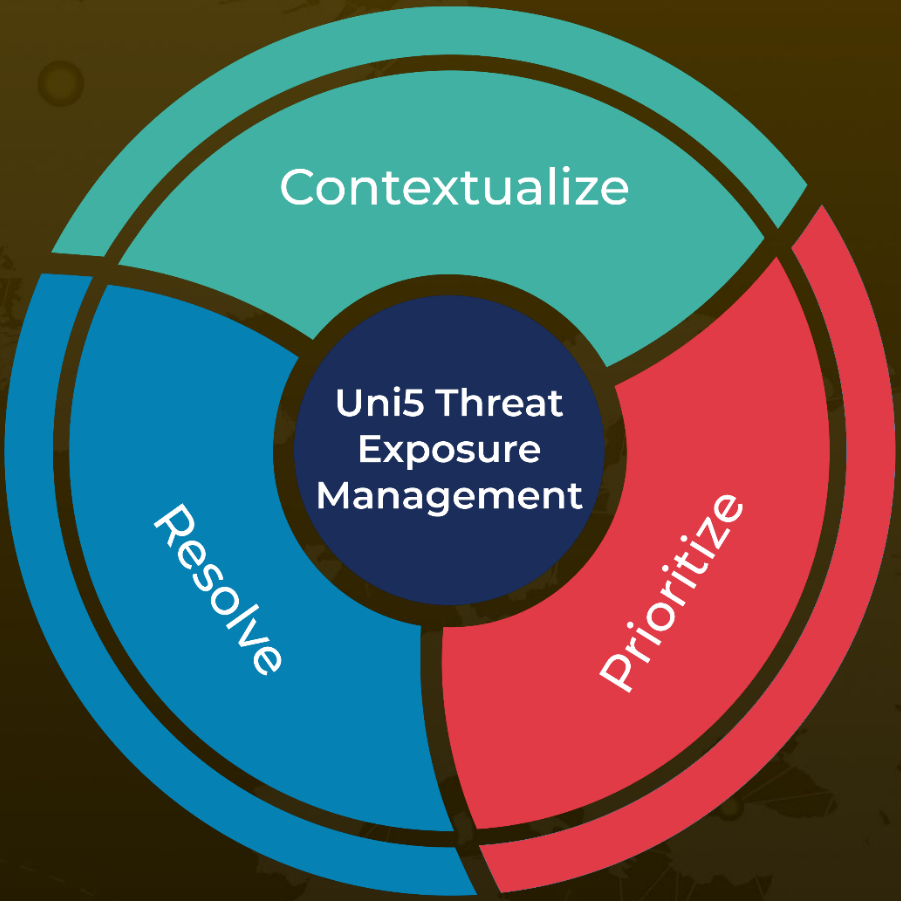
https://hivepro.com/threat-advisory/cve-2025-22457-hackers-actively-exploiting-ivantis-critical-new-flaw/

https://hivepro.com/threat-advisory/critical-cve-2025-31324-flaw-in-sap-netweaver-under-active-attack/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 26, 2025 • 11:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com