Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

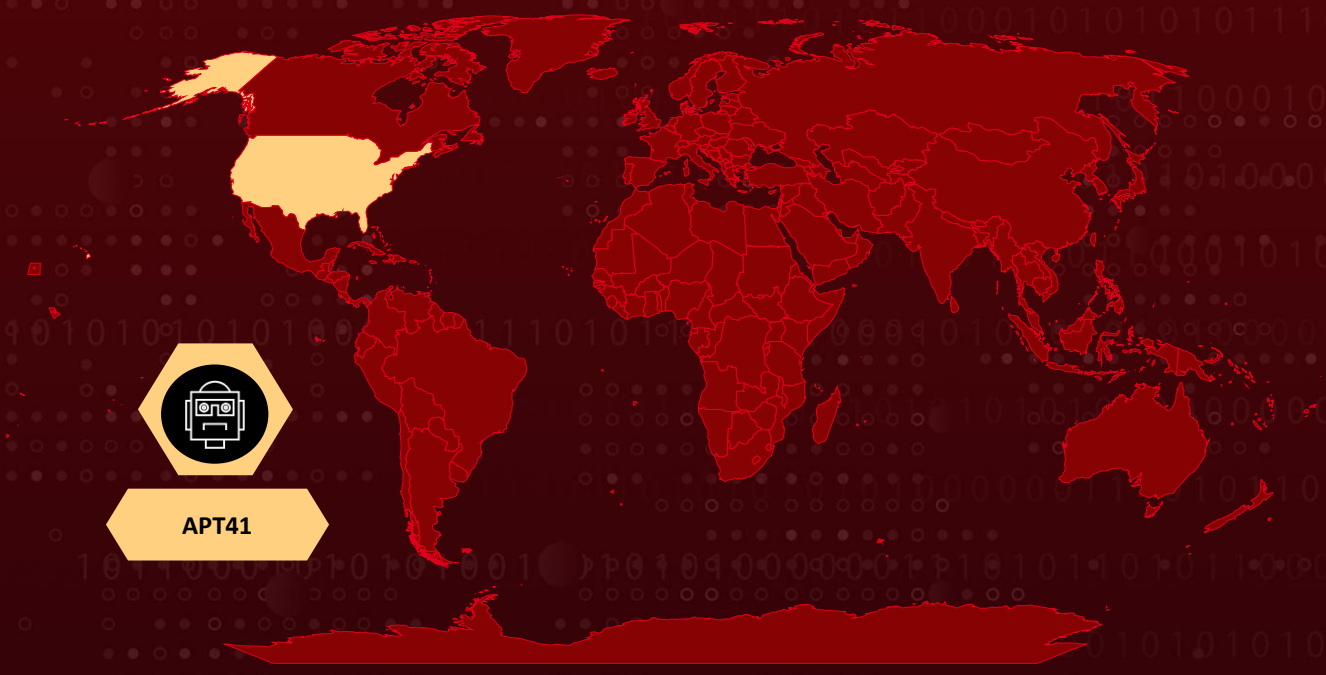
APT41 Cyber-Espionage Campaign Targets U.S. Policy Institutions

Date of Publication	Admiralty Code	TA Number
November 12, 2025	A1	TA2025342

Summary

First Seen: April 2025
Targeted Country: United States
Targeted Platform: Windows
Targeted Industries: Government, Non profit
Threat Actor: APT41 (aka HOODOO, WICKED PANDA, Winnti, Group 72, BARIUM, LEAD, GREF, Earth Baku, Brass Typhoon)
Malware: Deed RAT (aka Snappy Bee, Poisonplug.deed)
Attack: In April 2025, China-linked APT group APT41 launched a cyber-espionage campaign against a U.S. non-profit influencing government policy. The attackers exploited vulnerabilities such as Log4j and Atlassian OGNL Injection to gain access and used legitimate tools like msbuild.exe for stealthy persistence. They employed DLL sideloading with vetysafe.exe and deployed Deed RAT for remote access and credential theft. The operation reflects China's ongoing strategy to target policy institutions shaping U.S. foreign relations and highlights the need for stronger patching, monitoring, and threat-hunting defenses.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server/Data Center	✓	✓	✓
CVE-2021-44228	Log4Shell (Apache Log4j2 Remote Code Execution Vulnerability)	Apache Log4j2	✓	✓	✓
CVE-2017-9805	Apache Struts Deserialization of Untrusted Data Vulnerability	Apache Struts	✗	✓	✓
CVE-2017-17562	Embedthis GoAhead Remote Code Execution Vulnerability	Embedthis GoAhead	✗	✓	✓

Attack Details

#1

In April 2025, a coordinated cyber-espionage campaign was launched by the China-linked advanced persistent threat (APT) group APT41, with overlaps in tooling and techniques previously observed in Kelp (also known as Salt Typhoon) and Space Pirates operations. The operation targeted a U.S.-based non-profit organization involved in influencing government policy, underscoring the attackers' strategic focus on institutions that shape foreign policy and international relations. The campaign's objective was to gain long-term, covert access to the victim's network and exfiltrate sensitive policy-related intelligence.

#2

The intrusion began with extensive scanning for exploitable vulnerabilities, including Atlassian OGNL Injection (CVE-2022-26134), Log4j (CVE-2021-44228), Apache Struts (CVE-2017-9805), and GoAhead RCE (CVE-2017-17562). Once initial access was achieved, the attackers conducted internal reconnaissance to map network assets and confirm internet connectivity. They then created scheduled tasks under SYSTEM privileges to execute malicious code via legitimate binaries such as msbuild.exe, embedding payloads within XML configuration files. This "living-off-the-land" approach allowed malicious activity to blend in with routine administrative operations, helping the attackers remain undetected.

#3

A notable persistence method involved DLL sideloading, where a legitimate VipreAV executable (vetysafe.exe) signed by Sunbelt Software was used to load a malicious DLL (sbamres.dll). The campaign also employed Deed RAT (also known as Snappy Bee), a remote access trojan previously linked to Chinese threat groups. To escalate privileges and move laterally, the actors used techniques like DCSync to impersonate domain controllers and harvest credentials, as well as the Imjpuexc utility for obfuscation and persistence. These overlapping toolsets and methods are consistent with other Chinese APT operations, indicating a high degree of coordination and shared development.

#4

The operation demonstrated a high level of discipline and technical sophistication. Its focus on a policy-influencing organization reflects China's broader strategy of leveraging cyber operations to collect intelligence that can inform or anticipate U.S. foreign-policy decisions. The campaign underscores the ongoing threat posed by state-sponsored espionage and highlights the importance of continuous monitoring, proactive threat hunting, and timely patch management, particularly for institutions engaged in public policy, diplomacy, or strategic research.

Recommendations

Patch and Vulnerability Management: Immediately patch systems vulnerable to known exploited flaws, especially CVE-2022-26134, CVE-2021-44228 (Log4j), CVE-2017-9805, and CVE-2017-17562. Implement a robust vulnerability management program with continuous scanning and prioritized remediation of internet-facing services.

Hardening and Network Segmentation: Restrict access to administrative interfaces and sensitive systems through network segmentation and least-privilege principles. Limit lateral movement by separating critical infrastructure (e.g., domain controllers, policy data servers) from user networks.

Detection and Monitoring: Deploy advanced endpoint detection and response (EDR) solutions capable of identifying "living-off-the-land" techniques, scheduled task abuse, and DLL sideloading. Monitor for unusual process execution involving msbuild.exe, schtasks.exe, and netstat, especially under privileged accounts. Enable audit logging for task creation, registry changes, and DLL loads to improve visibility of persistence mechanisms.

Credential and Identity Security: Detect and mitigate DCSync or similar credential theft techniques by closely monitoring domain controller replication traffic. Enforce multi-factor authentication (MFA) for privileged and remote accounts. Regularly rotate administrative passwords and purge unused credentials or service accounts.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0007** Discovery
TA0005 Defense Evasion	**TA0011** Command and Control	**TA0010** Exfiltration	**TA0009** Collection
TA0006 Credential Access	**TA0008** Lateral Movement	**T1071** Application Layer Protocol	**T1059** Command and Scripting Interpreter
T1127.001 MSBuild	**T1082** System Information Discovery	**T1046** Network Service Discovery	**T1071.001** Web Protocols
T1127 Trusted Developer Utilities Proxy Execution	**T1053.005** Scheduled Task	**T1053** Scheduled Task/Job	**T1548** Abuse Elevation Control Mechanism
T1190 Exploit Public-Facing Application	**T1204** User Execution	**T1027** Obfuscated Files or Information	**T1059.001** PowerShell
T1574.002 DLL	**T1574** Hijack Execution Flow	**T1003.006** DCSync	**T1003** OS Credential Dumping
T1021 Remote Services	**T1219** Remote Access Software	**T1041** Exfiltration Over C2 Channel	**T1059.003** Windows Command Shell
T1588.006 Vulnerabilities	**T1588** Obtain Capabilities	**T1588.005** Exploits	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2561b457103e7e74f5e6d9dcf703bfe6, 96e3e845220da6795096bc37e3f82d6a
SHA1	0cd284f5e206972c66ba0eafe7a698fe7e9fc751, bcde791850b3a547aee585ea8c8bf060b16512a9
SHA256	51ffcff8367b5723d62b3e3108e38fb7cbf36354e0e520e7df7c8a4f52645c4d, 6f7f099d4c964948b0108b4e69c9e81b5fc5ff449f2fa8405950d41556850ed9, 99a0b424bb3a6bbf60e972fd82c514fd971a948f9cedf3b9dc6b033117ecb106, dae63db9178c5f7fb5f982fbd89683dd82417f1672569fef2bbfef83bec961e2, e356dbd3bd62c19fa3ff8943fc73a4fab01a6446f989318b7da4abf48d565af2, f52b86b599d7168d3a41182ccd89165e0d1f2562aa7363e0718d502b7e3fcb69
URL	hxxp[:]//38.180.83.166/6CDF0FC26CDF0FC2

Patch Links

https://www.atlassian.com/software/confluence/download-archives

https://logging.apache.org/security.html

https://cwiki.apache.org/confluence/display/WW/S2-052

https://github.com/advisories/GHSA-q5wm-274q-f3v6

References

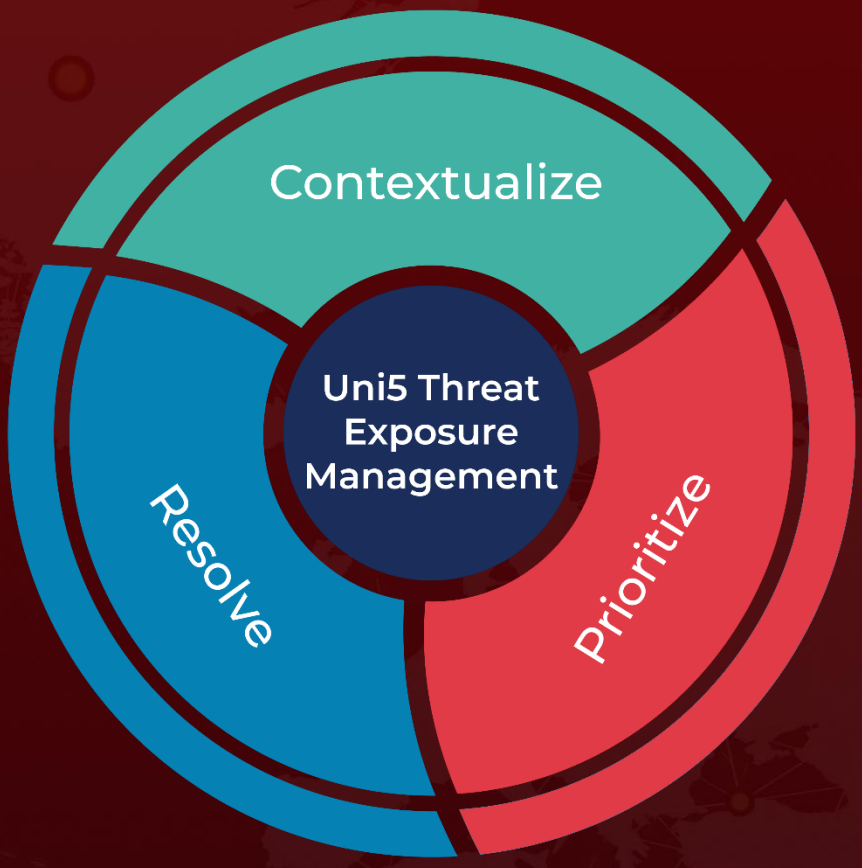
https://www.security.com/threat-intelligence/china-apt-us-policy

https://hivepro.com/threat-advisory/apt41-targets-african-government-it-services/

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

November 12, 2025 . 2:30 AM

More at www.hivepro.com