Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

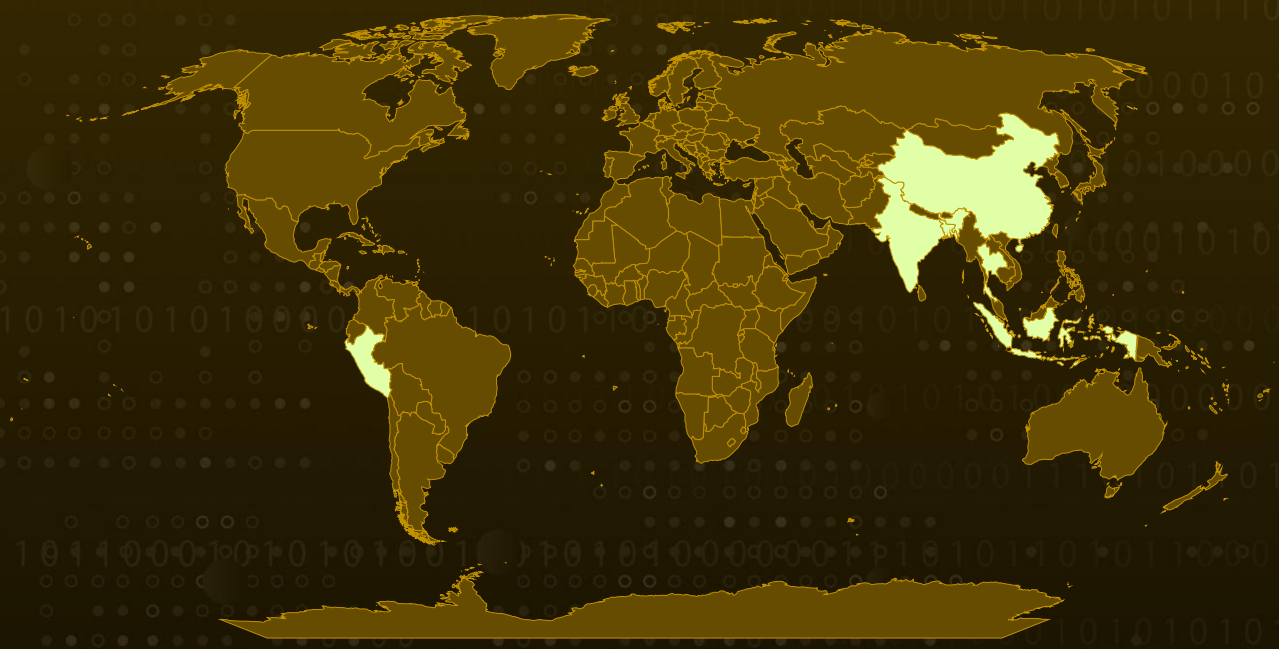
Web Traffic Hijacking via Malicious NGINX Configuration Injection

Date of Publication	Admiralty Code	TA Number
February 06, 2026	A1	TA2026037

Summary

First Seen: 2026
Targeted Regions: India, Indonesia, Peru, Bangladesh, Thailand, China
Targeted Platforms: Linux Servers, Containerized Environments
Targeted Industries: Government, Education, Web Hosting
Attack: Threat actors are actively conducting a web traffic hijacking campaign, likely exploiting the critical React2Shell vulnerability (CVE-2025-55182) to target vulnerable NGINX servers and Baota (BT) hosting management panels. The attackers tamper with NGINX configuration files to silently intercept and reroute legitimate website traffic through infrastructure they control, enabling traffic manipulation and further exploitation. The operation primarily targets Asian domains, including .in, .id, .pe, .bd, and .th, as well as Chinese hosting environments and sensitive sectors using government and educational domains. A multi-stage shell-based toolkit automates the entire operation, handling server compromise, configuration injection, persistence, and data exfiltration across infected systems.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

The campaign kicks off with attackers gaining a foothold on exposed NGINX servers, most likely by exploiting the critical React2Shell vulnerability (CVE-2025-55182). Once inside, they deploy an orchestrator script named zx.sh, which acts as the central loader for the attack chain. This script retrieves additional payloads using common utilities like curl or wget but also includes a fallback mechanism that leverages Bash's /dev/tcp feature to send HTTP requests directly if standard download tools are unavailable, ensuring the infection proceeds even in restricted environments.

#2

After securing access, the attackers deploy tailored scripts to modify NGINX configurations based on the server environment. One script, bt.sh, specifically targets systems running the Baota (BT) management panel, scanning configuration directories and injecting malicious location blocks that quietly proxy traffic to attacker-controlled servers. A more advanced script, 4zdh.sh, focuses on conventional NGINX installations, carefully editing configuration files across multiple directories while validating changes with nginx -t to avoid service disruption. Another variant, zdh.sh, concentrates on Linux and containerized deployments, applying targeted injections and forcefully restarting services if needed to ensure changes take effect.

#3

The injected configurations manipulate web traffic by redirecting selected requests through attacker infrastructure, with routing decisions made based on domain extensions. Government, education, and several Asian domains are funneled through one proxy network, while domains from regions like India and Indonesia are routed through another. A general fallback handles all remaining domains. To maintain stealth, the configuration preserves original request headers so redirected traffic appears legitimate. Only requests hitting predefined paths often resembling gaming, casino, blog, or support pages are redirected, reducing the chance of detection. Persistence is ensured through hash-based tracking files and careful configuration management that prevents repeated injections.

#4

In the final phase, a reconnaissance script gathers detailed information about all hijacked configurations and the relationships between compromised domains and attacker-controlled proxies. This data is then exfiltrated to a command-and-control server using authenticated requests, either through standard tools or direct TCP communication. Post-compromise activity also includes cryptomining deployment and reverse shells, showing that attackers aim not only to monetize resources automatically but also to retain interactive control over compromised systems.

Recommendations

Audit NGINX Configuration Files: Conduct immediate and comprehensive audits of all NGINX configuration files across managed infrastructure, specifically examining location blocks for unauthorized proxy_pass directives, unexpected rewrite rules, and unfamiliar backend domains.

Patch React2Shell Vulnerability (CVE-2025-55182): Prioritize patching all systems susceptible to the React2Shell vulnerability, as it is the primary initial access vector for this campaign. Verify patch status across all internet-facing servers running React-based applications.

Implement File Integrity Monitoring for NGINX Configurations: Deploy file integrity monitoring (FIM) rules that detect modifications to NGINX configuration files in directories such as /etc/nginx/, /usr/local/nginx/conf/, and /www/server/panel/vhost/nginx. Alert on any changes to files with the .conf extension in these paths.

Secure Baota (BT) Panel Deployments: Restrict access to Baota management panels to trusted IP addresses only, enforce strong authentication with multi-factor authentication, and ensure panels are updated to the latest version. Audit panel access logs for unauthorized login attempts or configuration changes.

Restrict Outbound Connectivity from Web Servers: Implement network segmentation and egress filtering to prevent web servers from initiating outbound connections to unauthorized external domains. NGINX servers should generally not need to establish connections to arbitrary external hosts.

Validate NGINX Configurations Before Reload: Implement automated configuration validation workflows that compare NGINX configurations against a known-good baseline before any reload or restart operation. Use version-controlled configuration management to detect unauthorized modifications.

Conduct Network Traffic Analysis: Perform deep packet inspection and network traffic analysis to identify anomalous proxy patterns where legitimate user traffic is being routed through unexpected intermediary servers. Look for discrepancies between expected and actual backend destinations.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Persistence	T1505: Server Software Component	T1505.004: IIS Components
Defense Evasion	T1027: Obfuscated Files or Information	
Discovery	T1083: File and Directory Discovery	
	T1082: System Information Discovery	
Collection	T1557: Adversary-in-the-Middle	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	xzz[.]pier46[.]com, ide[.]hashbank8[.]com, th[.]cogicpt[.]org
IPv4	158[.]94[.]210[.]227
File Path	/tmp/.domain_group_map.conf

References

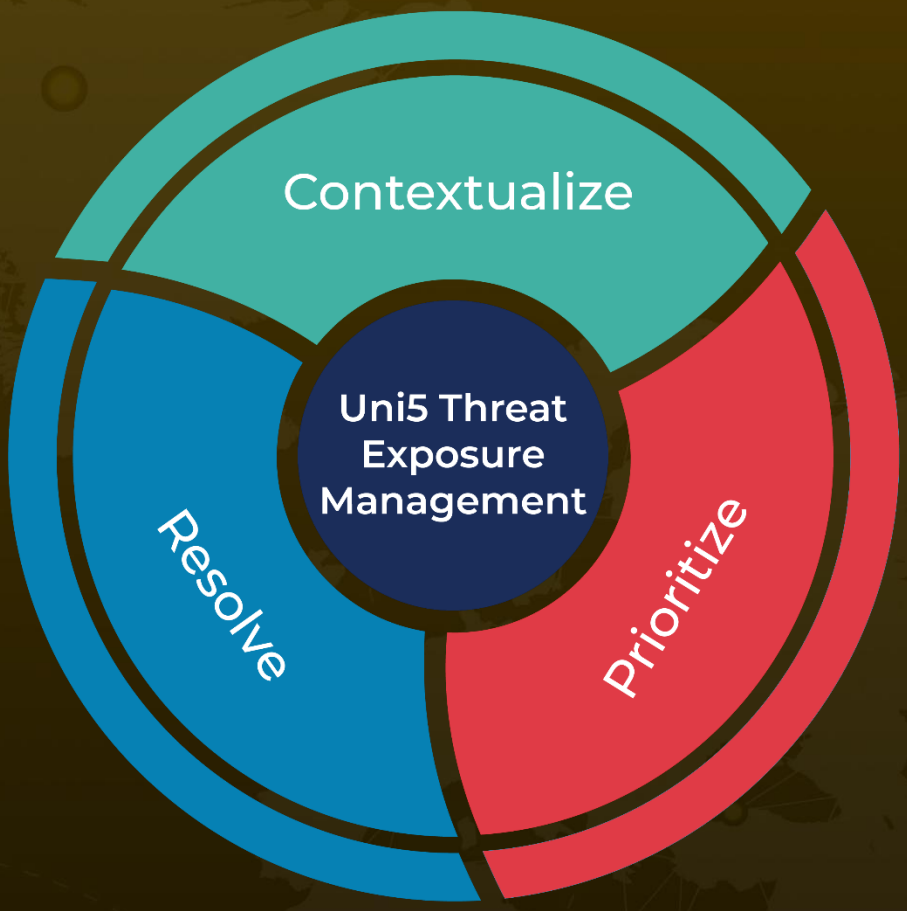
https://securitylabs.datadoghq.com/articles/web-traffic-hijacking-nginx-configuration-malicious/

https://hivepro.com/threat-advisory/react2shell-flaw-in-react-server-components-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

February 06, 2026 • 6:30 AM

More at www.hivepro.com