Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

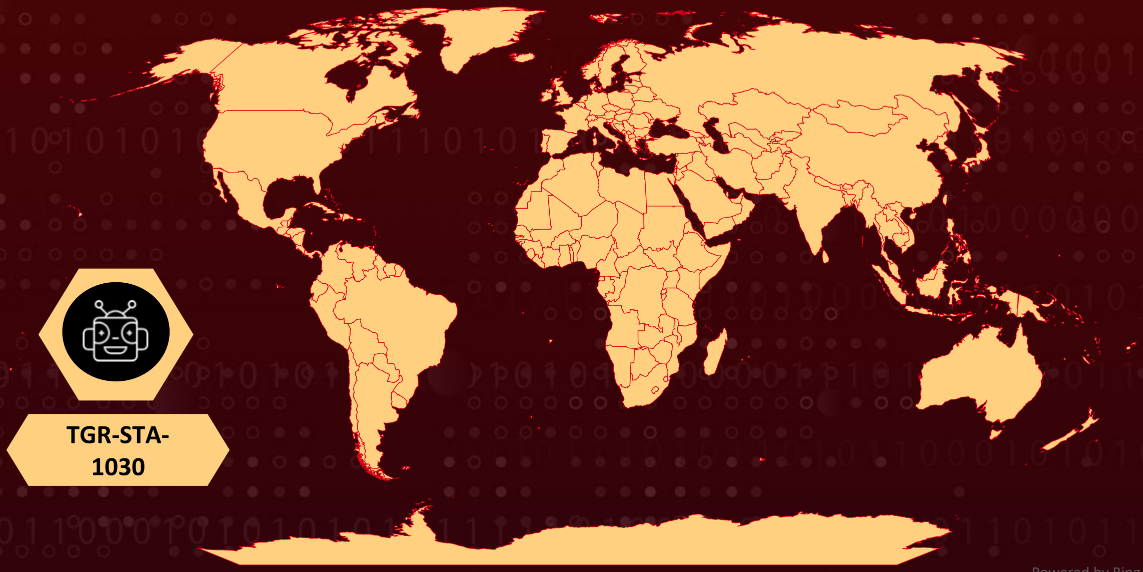
TGR-STA-1030: Global State-Aligned Cyber Espionage Campaign

Date of Publication	Admiralty Code	TA Number
February 10, 2026	A1	TA2026041

Summary

First Seen: January 2024
Targeted Regions: Worldwide
Targeted Platforms: Linux, Windows
Targeted Industries: Government, Foreign Affairs, Finance, Interior, Justice, Trade, Economy, Energy, Immigration, Mining, Natural Resources, Law Enforcement, Border Control, Counter-terrorism, Defense, Telecommunications, Aviation, Financial Services, Technology, Public Sector IT, Parliament, Diplomatic Services
Threat Actor: TGR-STA-1030 (aka UNC6619)
Malware: ShadowGuard, Diaoyu, VShell, Cobalt Strike, Havoc, Sliver, SparkRat
Campaign: Shadow Campaigns
Attack: TGR-STA-1030 (aka UNC6619) is a state-aligned cyberespionage group active since at least January 2024, assessed to operate primarily from Asia and focused on long-term intelligence collection. The group has compromised more than 70 organizations across 37 countries and conducted global reconnaissance against government infrastructure, primarily affecting government, diplomatic, law enforcement and critical infrastructure sectors. Initial access is achieved through spear-phishing and exploitation of known vulnerabilities, followed by deployment of custom loaders, advanced post-exploitation frameworks and a Linux eBPF kernel rootkit to maintain stealthy persistence. Targeting aligns closely with geopolitical, economic and military intelligence priorities, indicating sustained state-sponsored strategic collection.

Attack Regions



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

🟨 Targeted 🟥 Non-Targeted

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2019-11580	Atlassian Crowd and Crowd Data Center Remote Code Execution Vulnerability	Atlassian Crowd and Crowd Data Center	✗	✓	✓

Attack Details

#1

A state-aligned cyberespionage group designated TGR-STA-1030 (also tracked as UNC6619) has been active since at least January 2024 and is assessed to operate primarily from Asia, with activity patterns consistent with GMT+8 working hours. Over the past year, the group has compromised more than 70 organizations across 37 countries, targeting government ministries, law enforcement agencies, critical infrastructure and diplomatic institutions. Between November and December 2025, the group conducted focused reconnaissance against government infrastructure associated with 155 countries, selectively profiling specific entities rather than performing indiscriminate scanning.

#2

Initial access is achieved through a combination of spear-phishing and N-day vulnerability exploitation. Phishing campaigns use government-themed lures, including fabricated ministry reorganization notices, to deliver malicious archives hosted on mega.nz. These archives contain a custom loader, Diaoyu, which incorporates sandbox evasion techniques such as screen resolution checks and file dependency validation. The group also exploits publicly disclosed vulnerabilities affecting platforms including Microsoft Exchange, SAP, Apache Struts2 and Atlassian Crowd, demonstrating rapid adoption of proof-of-concept exploit code.

#3

Following compromise, TGR-STA-1030 employs a layered toolset to maintain persistence and enable lateral movement. The group has transitioned from Cobalt Strike to VShell, a Go-based command-and-control framework, while also leveraging Havoc, SparkRat and Sliver. Web shells such as Behinder, Godzilla and Neo-reGeorg are deployed on both external-facing and internal servers. Traffic is tunneled through GOST, FRPS and IOX, forming a multi-tiered infrastructure using VPS relays, residential proxies and Tor nodes. Victim-facing servers are frequently hosted in rule-of-law jurisdictions to blend in with legitimate traffic. The group also deploys a previously undocumented eBPF-based Linux kernel rootkit, ShadowGuard, which hides processes, conceals files and intercepts system calls.

#4 Targeting patterns align with strategic geopolitical and economic intelligence priorities, including rare earth mining, trade policy, diplomatic developments, and military-strategic interests across multiple regions. Given its scale, persistence and sophistication, TGR-STA-1030 represents a significant ongoing threat to government and critical infrastructure organizations worldwide.

Recommendations

Block Known Malicious Domains and Infrastructure: Immediately block the C2 domains gouvn[.]me, dog3rj[.]tech, zamstats[.]me, and 888910[.]xyz at the DNS and proxy level. Add all identified IP addresses and SHA-256 hashes from the IoC section to blocklists across endpoint detection, firewall, and SIEM platforms.

Patch Exploited Vulnerabilities Across Enterprise Software: Prioritize patching for all vulnerability classes exploited by TGR-STA-1030, including CVE-2019-11580 (Atlassian Crowd), Microsoft Exchange Server RCE, SAP Solution Manager privilege escalation, Microsoft Open Management Infrastructure RCE, and D-Link RCE vulnerabilities. Ensure all public-facing applications are current on security updates.

Scan for Web Shell Artifacts on External and Internal Servers: Conduct thorough scans for Behinder, Neo-reGeorg, and Godzilla web shells across all internet-facing and internal web servers. Look for obfuscated variants using Tas9er-style techniques with function and string names referencing "Baidu."

Hunt for ShadowGuard eBPF Rootkit Indicators on Linux Systems: On Linux systems, check for the presence of files or directories containing "swsecret," unexpected eBPF programs loaded in the kernel, and anomalies in process listings where known running services do not appear. Use tools capable of enumerating loaded eBPF programs such as bpftool to detect unauthorized kernel-level instrumentation.

Enhance Email Security Against Localized Phishing Lures: Strengthen email gateway controls to detect and quarantine archive files (.zip) linked from Mega.nz and other cloud storage providers. Implement heuristic analysis for executables within archives that perform environment checks (screen resolution validation, file dependency verification) as anti-sandbox techniques.

Monitor for Anomalous Tunneling and C2 Activity: Deploy detection rules for GOST, FRPS, and IOX tunneling tools on internal networks. Monitor for outbound connections on 5-digit ephemeral TCP ports characteristic of VShell C2 configurations, as well as SSH on unusual high-numbered ports and unexpected RDP sessions on port 3389.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
	T1190: Exploit Public-Facing Application	
Execution	T1204: User Execution	T1204.002: Malicious File
Defense Evasion	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1014: Rootkit	
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
Persistence	T1505: Server Software Component	T1505.003: Web Shell
Command and Control	T1105: Ingress Tool Transfer	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1572: Protocol Tunneling	
	T1090: Proxy	T1090.002: External Proxy
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.003: Virtual Private Server
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	66ec547b97072828534d43022d766e06c17fc1cafe47fbd9d1ffc22e2d52a9c0, 23ee251df3f9c46661b33061035e9f6291894ebe070497ff9365d6ef2966f7fe, 5175b1720fe3bc568f7857b72b960260ad3982f41366ce3372c04424396df6fe, 358ca77ccc4a979ed3337aad3a8ff7228da8246eebc69e64189f930b325daf6a, 293821e049387d48397454d39233a5a67d0ae06d59b7e5474e8ae557b0fc5b06, c876e6c074333d700adf6b4397d9303860de17b01baa27c0fa5135e2692d3d6f, b2a6c8382ec37ef15637578c6695cb35138ceab42ce4629b025fa4f04015eaf2, 5ddeff4028ec407ffdaa6c503dd4f82fa294799d284b986e1f4181f49d18c9f3, 182a427cc9ec22ed22438126a48f1a6cd84bf90fddb6517973bcb0bac58c4231, 7808b1e01ea790548b472026ac783c73a033bb90bbe548bf3006abfbcb48c52d, 9ed487498235f289a960a5cc794fa0ad0f9ef5c074860fea650e88c525da0ab4
Domains	abwxjp5[.]me, brackusi0n[.]live, dog3rj[.]tech, emezonhe[.]me, gouvn[.]me, msonline[.]help, pickupweb[.]me, pr0fu5a[.]me, q74vn[.]live, servgate[.]me, zamstats[.]me, zrheblirsy[.]me

TYPE	VALUE
IPv4	138[.]197[.]44[.]208, 142[.]91[.]105[.]172, 146[.]190[.]152[.]219, 157[.]230[.]34[.]45, 157[.]245[.]194[.]54, 159[.]65[.]156[.]200, 159[.]203[.]164[.]101, 178[.]128[.]60[.]22, 178[.]128[.]109[.]37, 188[.]127[.]251[.]171, 188[.]166[.]210[.]146, 208[.]85[.]21[.]30
URLs	hxxps[:]//raw.githubusercontent[.]com/padeqav/WordPress/refs/heads/master/wp-includes/images/admin-bar-sprite[.]png, hxxps[:]//raw.githubusercontent[.]com/padeqav/WordPress/refs/heads/master/wp-includes/images/Linux[.]jpg, hxxps[:]//raw.githubusercontent[.]com/padeqav/WordPress/refs/heads/master/wp-includes/images/Windows[.]jpg

Patch Details

https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html

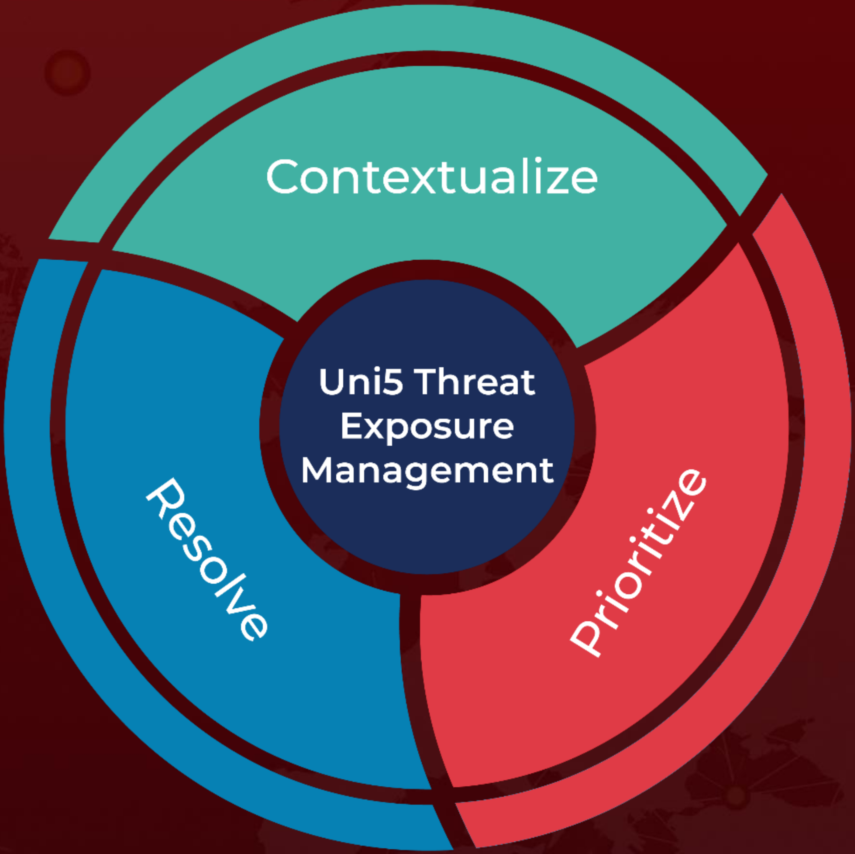
References

https://unit42.paloaltonetworks.com/shadow-campaigns-uncovering-global-espionage/

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 10, 2026 • 6:30 AM

More at www.hivepro.com