JEDI SECURITY

Threat Assessment Profile

Subject: TGR-STA-1030 ("Shadow Campaigns")

Date: February 9, 2026 (America/Chicago)

Version: v1.0

Overall Risk: HIGH (global espionage, persistent access, kernel-level stealth)

This profile summarizes publicly reported activity attributed by Palo Alto Networks Unit 42 to a previously undocumented espionage cluster tracked as TGR-STA-1030. It is intended for defenders and incident responders.

Key Finding	Detail
Scope	At least 70 government and critical infrastructure organizations compromised across 37 countries.
Reconnaissance	Scanning/targeting of government-linked infrastructure associated with 155 countries (Nov–Dec 2025).
Initial Access	Tailored phishing + exploitation of known ("N-day") vulnerabilities; no evidence of zero-days in reporting.
Notable Capability	Custom Linux kernel eBPF rootkit ("ShadowGuard") enabling stealth (process/file hiding).
Primary Motive (assessed)	Strategic / economic / political intelligence collection (espionage).

Analyst Note: Attribution is reported as "state-aligned" and "operating out of Asia" without naming a specific government. Defenders should focus on observed behaviors and exposure reduction.

Executive Summary

Unit 42 describes "Shadow Campaigns" as a large-scale, operationally mature espionage effort that compromised government and critical infrastructure organizations across 37 countries. Public reporting emphasizes two parallel access paths: targeted phishing with localized lures, and exploitation of known vulnerabilities in widely deployed enterprise products. Once inside, the operator established persistence, moved laterally, and used a mix of commodity and bespoke tooling including a Linux kernel eBPF rootkit ("ShadowGuard") for stealth.

- **Who should care:** Governments, critical infrastructure operators, enterprises with internet-facing email/ERP/collaboration platforms, and orgs in sectors tied to trade, energy, mining, elections, telecom, and finance.
- **What makes it dangerous:** Global scale, persistence, diverse tooling (webshells/tunnels/C2 frameworks), and kernel-level hiding on Linux.
- **Defensive priority:** Patch/mitigate exploited N-day exposures, harden email security, restrict and monitor egress, and improve Linux visibility (incl. eBPF controls) on high-value systems.

Confidence: High for reported scope and TTPs (multiple independent reports citing Unit 42). Moderate for precise targeting motives (inferred from timing/targets).

Threat Actor Profile

Identity and Attribution

Tracked by Unit 42 as **TGR-STA-1030** (also reported alongside the identifier **UNC6619** in some coverage). Unit 42 assesses with high confidence that the cluster is **state-aligned** and **operates out of Asia**. Public sources do not provide definitive attribution to a named country or agency.

Operational Timeline and Objectives

Activity is described as active since at least **January 2024**. The campaign appears oriented toward strategic intelligence collection, with multiple reports emphasizing economic, diplomatic, and political interests based on victim sectors and event-driven targeting.

Targeting Highlights

- Government ministries: finance, interior, foreign affairs, trade/economy, immigration, natural resources/mining, energy.
- Law enforcement and border control entities.
- National telecom and other critical infrastructure providers.
- Event-driven targeting tied to elections and geopolitical developments (reported in open sources).

Risk Assessment (Defender View)

Dimension	Assessment	Rationale (public reporting)
Likelihood	High	Large-scale scanning plus confirmed compromises across many regions indicates continued opportunity.
Impact	High	Espionage on government/critical infrastructure; persistence and kernel-level stealth can prolong dwell time.
Detectability	Medium–Low	Use of webshells/tunnels plus ShadowGuard rootkit can reduce host-based visibility.

Observed Tactics, Techniques, and Procedures

Initial Access

Reporting describes two primary entry methods: (1) tailored phishing emails that deliver a loader via cloud storage, and (2) exploitation of known vulnerabilities ("N-day"), with no public evidence of zero-day use in this campaign.

Phishing path (high-level):

- Email lures referencing internal ministry topics and reorganization efforts (localized to the target).
- Links to archives hosted on MEGA (mega.nz) containing the Diaoyu loader and a zero-byte file named **pic1.png** (integrity check).
- Environment checks (screen resolution and security product process checks) before pulling additional payloads (e.g., Cobalt Strike / VShell).

N-day exploitation path (high-level):

- Attempts against multiple enterprise and infrastructure products were reported (examples include Microsoft Exchange/Windows, SAP Solution Manager, Atlassian, and others).
- Emphasis is on opportunistic exploitation of already-known security issues rather than novel exploit development.

Post-Compromise Tooling

Open reporting lists a broad toolkit spanning C2 frameworks, web shells, and tunneling utilities. The mix suggests flexibility across Windows and Linux environments and a preference for reliable, operator-friendly tradecraft rather than stealth-only bespoke malware.

- **C2 frameworks:** Cobalt Strike, VShell, Havoc, Sliver, SparkRAT (reported).
- **Web shells:** Behinder, Godzilla, neo-reGeorg (reported).
- **Tunneling / proxy:** GOST, FRPS, IOX; plus relay infrastructure and proxy services (reported).

Kernel-Level Stealth (Linux)

Multiple reports cite a custom Linux kernel eBPF rootkit called **ShadowGuard**. It is described as hiding selected processes (PIDs) and concealing files/directories named **swsecret**, complicating detection using standard userland tools.

Detection and Mitigation Guidance

Fast Triage Checklist (24–72 hours)

- **Patch exposure first:** Identify and remediate internet-facing systems in the product families cited in public reporting (email, ERP/management platforms, collaboration tooling, edge/network devices).
- **Hunt for the phishing tradecraft:** MEGA-hosted archives, unusual localized archive names, presence of **pic1.png** (0-byte) alongside unexpected executables, and execution from user download directories.
- **Control outbound traffic:** Review and restrict outbound where feasible; baseline and alert on new outbound tunnels/proxy behavior from servers (unexpected FRP/GOST-like patterns).
- **Linux visibility upgrade:** On high-value Linux servers, collect kernel/audit telemetry and consider restricting unprivileged eBPF where compatible with your workload.
- **Persistence review:** Inspect for new scheduled tasks/services, new SSH keys, webshell paths under web roots, and suspicious reverse proxy configs.

Detection Opportunities by Stage

Stage	What to Log / Watch	Why it Helps
Email / Phishing	Attachment/URL telemetry; MEGA links; rare archive names; download-to-exec patterns	Catches initial loader delivery and user-driven execution.
Execution	Endpoint process creation; parent/child chains; execution from user profile dirs	Flags loader behavior and early staging.
Privilege / Persistence	New services, scheduled tasks, autoruns; new local admins; SSH key additions	Common steps to maintain access.
Webshells	Web server access logs; new/modified web files; unusual POST patterns	Webshell traffic often leaves distinct server log traces.
Tunneling / C2	Netflow/DNS logs; long-lived outbound connections; unusual ports; VPS endpoints	Espionage ops depend on stable outbound channels.
Linux rootkit signals	Kernel/audit anomalies; hidden PID discrepancies; integrity monitoring around 'swsecret' paths	ShadowGuard is designed to evade userland tools.

IOC Note: Unit 42 and downstream reporting reference published indicators of compromise (domains/IPs/hashes). Given IOC churn, prioritize behavioral detection and exposure reduction; ingest vendor IOCs into detection tooling as a supplement.

Appendix A: High-Level MITRE ATT&CK; Mapping (Representative)

Tactic	Technique (examples)	Notes (public reporting)
Initial Access	Spearphishing Link (T1566.002)	Phishing emails deliver MEGA-hosted archives and loader.
Initial Access	Exploit Public-Facing Application (T1190)	Use of known vulnerabilities in enterprise products.
Execution	User Execution (T1204)	User opens/executes malicious archive contents.
Defense Evasion	Obfuscated/Compressed Files (T1027)	Archive-based delivery; staging via cloud storage.
Defense Evasion	Rootkit (T1014)	Linux eBPF rootkit ShadowGuard for stealth.
Persistence	Web Shell (T1505.003)	Behinder/Godzilla/neo-reGeorg reported.
Command and Control	Web Protocols (T1071.001)	C2 frameworks typically use HTTP/S.
Command and Control	Remote Services / Tunneling	FRP/GOST/IOX-style tunneling and relay infrastructure.
Collection	Email Collection (varies)	Open reporting emphasizes interest in email infrastructure and sensitive documents.

Appendix B: References (Public Sources)

1 Palo Alto Networks Unit 42. “The Shadow Campaigns: Uncovering Global Espionage.” Published February 5, 2026. https://unit42.paloaltonetworks.com/shadow-campaigns-uncovering-global-espionage/

2 The Hacker News (Ravie Lakshmanan). “Asian State-Backed Group TGR-STA-1030 Breaches 70 Government, Infrastructure Entities.” February 6, 2026. https://thehackernews.com/2026/02/asian-state-backed-group-tgr-sta-1030.html

3 Axios (Sam Sabin). “Hackers breach 37 countries in ongoing espionage campaign.” February 5, 2026. https://www.axios.com/2026/02/05/cyberespionage-government-hacking-campaign-palo-alto-networks

4 BleepingComputer (Bill Toulas). “State actor targets 155 countries in ‘Shadow Campaigns’ espionage op.” February 7, 2026. https://www.bleepingcomputer.com/news/security/state-actor-targets-155-countries-in-shadow-campaigns-espionage-op/