# The Shadow Campaigns: Uncovering Global Espionage

By Unit 42

Published: 2026-02-05 · Archived: 2026-04-05 18:01:52 UTC

## Executive Summary

This investigation unveils a new cyberespionage group that Unit 42 tracks as TGR-STA-1030. We refer to the group's activity as the Shadow Campaigns. We assess with high confidence that TGR-STA-1030 is a state-aligned group that operates out of Asia. Over the past year, this group has compromised government and critical infrastructure organizations across 37 countries. This means that approximately one out of every five countries has experienced a critical breach from this group in the past year. Further, between November and December 2025, we observed the group conducting active reconnaissance against government infrastructure associated with 155 countries.

This group primarily targets government ministries and departments. For example, the group has successfully compromised:

- Five national-level law enforcement/border control entities
- Three ministries of finance and various other government ministries
- Departments globally that align with economic, trade, natural resources and diplomatic functions

Given the scale of compromise and the significance of these organizations, we have notified impacted entities and offered them assistance through responsible disclosure protocols.

Here we describe the technical sophistication of the actors, including the phishing and exploitation techniques, tooling and infrastructure used by the group. We provide defensive indicators to include infrastructure that is active at the time of this publication. Further, we explore an in-depth look at victimology by region with the intent of demonstrating the suspected motivations of the group. The results indicate that this group prioritizes efforts against countries that have established or are exploring certain economic partnerships.

Additionally, we have also pre-shared these indicators with industry peers to ensure robust cross-industry defenses against this threat actor.

Palo Alto Networks customers are better protected from the threats described in this article through products and services, including:

- Advanced URL Filtering and Advanced DNS Security
- Advanced WildFire
- Advanced Threat Prevention
- Cortex XDR and XSIAM
- If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

## Actor Introduction

Unit 42 first identified TGR-STA-1030 (aka UNC6619) upon investigating a cluster of malicious phishing campaigns (referred to here as the Shadow Campaigns) targeting European governments in early 2025. We use the prefix TGR-STA as a placeholder to denote a temporary group of state-aligned activity while we continue to refine attribution to a specific organization.

Since our initial investigation, we have identified actor infrastructure dating as far back as January 2024, suggesting that the group has been active for at least two years. Over the past year, we have monitored the evolution and expansion of the group as it has compromised:

- Five national-level law enforcement/border control entities
- Three ministries of finance and various other government ministries
- Departments globally that align with economic, trade, natural resources and diplomatic functions

We assess with high confidence that TGR-STA-1030 is a state-aligned group that operates out of Asia. We base this assessment on the following findings:

- Frequent use of regional tooling and services
- Language setting preferences
- Targeting and timing that routinely align with events and intelligence of interest to the region
- Upstream connections to operational infrastructure originating from the region
- Actor activity routinely aligning with GMT+8

Additionally, we found that one of the attackers uses the handle “JackMa,” which could refer to the billionaire businessman and philanthropist who co-founded Alibaba Group and Yunfeng Capital.

## Phishing

In February 2025, Unit 42 investigated a cluster of malicious phishing campaigns targeting European governments. These campaigns followed a pattern of being sent to government email recipients with a lure of a ministry or department reorganization and links to malicious files hosted on mega[.]nz. Figure 1 below shows an example.

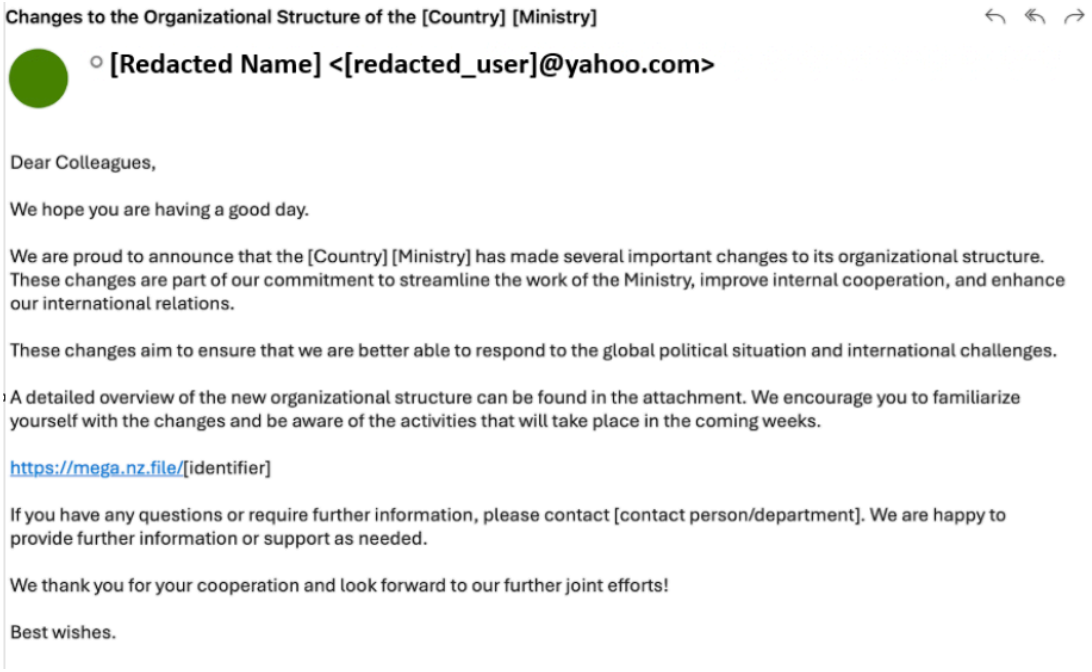


Figure 1. Example phishing email (translated).

Clicking on the link downloads an archive file with language and naming that is consistent with the targeted country and ministry.

We assess that an Estonian government entity identified the campaign and uploaded one such ZIP archive to a public malware repository. In this case, the Estonian filename was:

Politsei- ja Piirivalveameti organisatsiooni struktuuri muudatused.zip

This translates to Changes to the organizational structure of the Police and Border Guard Board.zip

## Diaoyu Loader

Analyzing the archive, we found that the contents were last modified on Feb. 14, 2025. Further, the archive itself contains an executable file containing an identical name as the ZIP and a zero-byte file named pic1.png.

Reviewing the executable metadata, we found that the file version is presented as 2025,2,13,0, suggesting that the file was likely created one day prior, on Feb. 13. This date also corresponds to the PE compile timestamp.

Additionally, the metadata shows that the file's original name was DiaoYu.exe. The term Diaoyu translates to fishing, or phishing in a cybersecurity context.

The malware employs a dual-stage execution guardrail to thwart automated sandbox analysis. Beyond the hardware requirement of a horizontal screen resolution greater than or equal to 1440, the sample performs an environmental dependency check for a specific file (pic1.png) in its execution directory.

In this context, pic1.png acts as a file-based integrity check. If the malware sample is submitted to a sandbox in isolation, the absence of this auxiliary file causes the process to terminate gracefully before detonation, effectively masking its malicious behavior. Only upon satisfying these prerequisites does the malware proceed to audit the host for the following cybersecurity products:

- Avp.exe (Kaspersky)
- SentryEye.exe (Avira)
- EPSecurityService.exe (Bitdefender)
- SentinelUI.exe (Sentinel One)
- NortonSecurity.exe (Symantec)

This narrow selection of products is interesting, and it is unclear why the actor chose to only look for these specific products. While various malware families commonly check for the presence of antivirus products, malware authors typically include a more comprehensive list that encompasses a variety of global providers.

After checking for these products, the malware downloads the following files from GitHub:

- 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

It should be noted that the padeqav GitHub project is no longer available.

Finally, the malware performs a series of actions on these files that ultimately result in the installation of a Cobalt Strike payload.

## Exploitation

In addition to phishing campaigns, the group often couples exploitation attempts with their reconnaissance activities to gain initial access to target networks. To date, we have not observed the group developing, testing or deploying any zero-day exploits. However, we assess that the group is comfortable testing and deploying a wide range of common tools, exploitation kits and proof-of-concept code for N-day exploits.

For example, over the past year, our Advanced Threat Prevention service has detected and blocked attempts by the group to exploit the following types of vulnerabilities:

- SAP Solution Manager privilege escalation vulnerability
- Pivotal Spring Data Commons remote file read XXE vulnerability
- Microsoft Open Management Infrastructure remote code execution vulnerability
- Microsoft Exchange Server remote code execution vulnerability
- D-Link remote code execution vulnerability
- HTTP directory traversal request attempt
- HTTP SQL injection attempt
- Struts2 OGNL remote code execution vulnerability
- Ruijieyi Networks remote command execution vulnerability
- Eyou Email System remote command execution vulnerability
- Beijing Grandview Century eHR Software SQL injection vulnerability

- Weaver Ecology-OA remote code execution vulnerability
- Microsoft Windows win.ini access attempt detected
- Commvault CommCell CVSearchService download file authentication bypass vulnerability
- Zhiyuan OA remote code execution vulnerability

On one occasion, we observed the actor connecting to e-passport and e-visa services associated with a ministry of foreign affairs. Because the server for these services was configured with Atlassian Crowd software, the actor attempted to exploit CVE-2019-11580, uploading a payload named rce.jar. The code included in the payload was similar to the description of code from another analysis of CVE-2019-11580 provided by Anquanke.

## Tooling

We assess that the group relies heavily on a mix of command-and–control (C2) frameworks and tools common to the actors' region to move laterally and maintain persistent access within compromised environments.

### C2 Frameworks

From 2024 through early 2025, we observed the group commonly deploying Cobalt Strike payloads. However, over time the group slowly transitioned to VShell as its tool of choice.

VShell is a Go-based C2 framework. The group often configures its web access on 5-digit ephemeral TCP ports using ordered numbers. In November 2025, NVISO published comprehensive research [PDF] on the origins of this tool, its features and its wide-scale use by multiple threat groups and actors.

Within the past year, we assess that the group has also leveraged frameworks like Havoc, SparkRat and Sliver with varying degrees of success.

### Web Shells

TGR-STA-1030 has frequently deployed web shells on external-facing web servers as well as on internal web servers to maintain access and enable lateral movement. The three most common web shells used by the group are Behinder, Neo-reGeorg and Godzilla.

Further, we noted during one investigation that the group attempted to obfuscate its Godzilla web shells using code from the Tas9er GitHub project. This project obfuscates code by creating functions and strings with names like Baidu. It also adds explicit messages to governments.

### Tunnels

We have observed the group leveraging GO Simple Tunnel (GOST), Fast Reverse Proxy Server (FRPS), and IOX across both their C2 infrastructure and compromised networks to tunnel desired network traffic.

### Introducing ShadowGuard

During an investigation, we identified the group using a new Linux kernel rootkit, ShadowGuard. The sample we discovered (SHA-256 hash

7808B1E01EA790548B472026AC783C73A033BB90BBE548BF3006ABFBCB48C52D) is an Extended Berkeley Packet Filter (eBPF) rootkit designed for Linux systems. At this time, we assess that the use of this rootkit is unique to this group.

eBPF backdoors are notoriously difficult to detect because they operate entirely within the highly trusted kernel space. eBPF programs do not appear as separate modules. Instead, they execute inside the kernel's BPF virtual machine, making them inherently stealthy. This allows them to manipulate core system functions and audit logs before security tools or system monitoring applications can see the true data.

This backdoor leverages eBPF technology to provide the following kernel-level stealth capabilities:

- **Kernel-level concealment:** It can conceal process information details directly at the kernel level.
- **Process hiding (syscall interception):** The tool intercepts critical system calls, specifically using custom kill signals (entry and exit points) to identify which processes the attacker wants to hide.
    - It conceals specified process IDs (PIDs), making them invisible to standard user-space analysis tools like the standard Linux ps aux command
    - It can hide up to 32 processes simultaneously
- **File and directory hiding:** It features a hard-coded check to specifically conceal directories and files named swsecret.
- **Allow-listing:** The backdoor includes an allow list mechanism where processes placed on the list are deliberately excluded and remain unaffected by the hiding functionality.

When started, the program will automatically check for the following:

- Root privileges
- eBPF support
- Tracepoint support

Example commands once ShadowGuard is started are shown below in Table 1.

| **Command** | **Overview** |
|---|---|
| kill -900 1234 | -900 = Add target PID (1234) to the allow list |
| kill -901 1234 | -901 = Remove target PID (1234) from the allow list |
| touch swsecret_config.txt<br><br>mkdir swsecret_data<br><br>* Note: By default ShadowGuard hides/conceals any directories or files named swsecret. This could be a shortened, internal code name used by the rootkit's developers to tag their own files. Example: “Put all configuration and logs inside a directory named swsecret.” | ls -la files/directories beginning with swsecret should display as a dot . (i.e., it should be hidden) |

Table 1. Examples of commands for ShadowGuard.

## Infrastructure

Consistent with any advanced actor conducting cyberespionage, this group goes to great lengths to mask and obfuscate the origin of its operations. However, despite all of its best efforts, it is exceptionally hard to overcome the following two challenges:

1. Network Traffic Inspection: It is widely known that several nations employ methods to censor and filter traffic entering/exiting their respective countries. As such, it is extremely unlikely that foreign cyberespionage groups would willingly route their network traffic through any nation that employs these inspection capabilities.
2. Network evolution: Maintaining infrastructure for cyberespionage operations is hard. It requires the routine creation of new domains, virtual private servers (VPS) and network tunnels. Studying a group's infrastructure over time almost always reveals mistakes and errors where tunnels collapse or perhaps identity protection services expire.

### Network Structure

We assess that the group applies a multi-tiered infrastructure approach to obfuscate its activities.

#### Victim-Facing

The group routinely leases and configures its C2 servers on infrastructure owned by a variety of legitimate and commonly known VPS providers. However, unlike most groups that configure their malicious infrastructure on bulletproof providers or in obscure locations, this group prefers to establish its infrastructure in countries that have a strong rule of law.

For example, the group frequently chooses virtual servers in the U.S., UK and Singapore. We assess this preference in locations likely aids the group in three ways:

1. Infrastructure may appear more legitimate to network defenders
2. This could enable low-latency connections across the Americas, Europe and Southeast Asia
3. These locations have separate laws, policies and priorities that govern the operations of their domestic law enforcement and foreign intelligence organizations. Thus, having infrastructure in these locations likely necessitates cross-agency cooperation efforts for their governments to effectively investigate and track the group.

#### Relays

To connect to the C2 infrastructure, the group leases additional VPS infrastructure that it uses to relay traffic through. These hosts are often configured with SSH on port 22 or a high-numbered ephemeral port. In some cases, we have also observed hosts configured with RDP on port 3389.

#### Proxies

Over time, the group has leveraged a variety of capabilities to anonymize its connections to the relay infrastructure. In early 2025, we observed the group using infrastructure we associated with DataImpulse, a company that provides residential proxy services. Since then, we have observed the group using the Tor network and other proxy services.

**Upstream**

In tracking upstream infrastructure, it is important to recognize that the primary goal of an espionage group is to steal data. To accomplish that task, a group has to build a path from the compromised network back to a network it can access. As such, the flow of data upstream typically correlates geographically to the group's physical location.

As noted above, the act of maintaining all of this infrastructure and its associated connections is quite challenging. On occasion, the group makes mistakes either because it forgets to establish a tunnel or because a tunnel collapses. When this happens, the group connects directly from its upstream infrastructure.

On several occasions, we have observed the group connecting directly to relay and victim-facing infrastructure from IP addresses belonging to Autonomous System (AS) 9808. These IP addresses are owned by an internet service provider in the group's region.

## Domains

We have identified several domains used by the group to facilitate malware C2 communications. Most were registered with the following top-level domains:

- me
- live
- help
- tech

Noteworthy domains include:

- gouvn[.]me

The group used this domain to target Francophone countries that use gouv to denote government domains. While the actor consistently pointed this domain name to leased victim-facing VPS infrastructure, we noted an anomaly in late 2024. While the domain never pointed to it, the actor appears to have copied an X.509 certificate with the common name gouvn[.]me from a victim-facing VPS to a Tencent server located in the actors' region. Here it was visible for four days in November 2024.

- dog3rj[.]tech

The group used this domain to target European nations. It's possible that the domain name could be a reference to "DOGE Jr," which has several meanings in a Western context, such as the U.S. Department of Government Efficiency or the name of a cryptocurrency. This domain was registered using an email address associated with the domain 888910[.]xyz.

- zamstats[.]me

The group used this domain to target the Zambian government.

## Global Targeting Overview

Over the course of the past year the group has substantially increased its scanning and reconnaissance efforts. This shift follows the group's evolution from phishing emails to exploits for initial access. Most emblematic of this activity, we observed the group scanning infrastructure across 155 countries between November and December 2025, as noted in Figure 2.

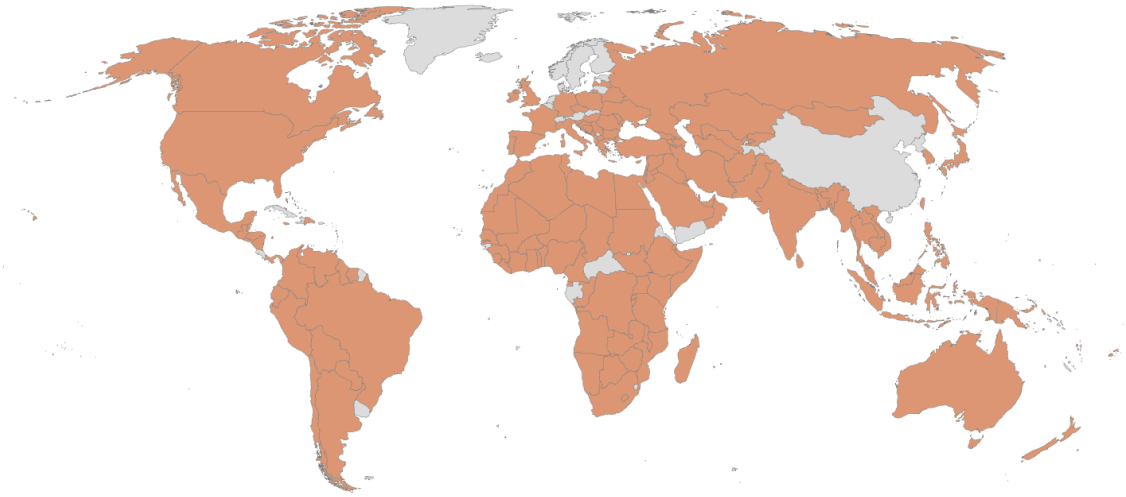

Figure 2. Countries targeted by TGR-STA-1030 reconnaissance between November and December 2025.

Given the expansive nature of the activity, some analysts might wrongly assume that the group simply launches broad scans across the entire IPv4 space from 1.1.1[.]1 to 255.255.255[.]255, but that is not the case. Based on our observation, the group focuses its scanning narrowly on government infrastructure and specific targets of interest across each country.

The group’s reconnaissance efforts shed light on its global interests. We have also observed the group's success at compromising several government and critical infrastructure organizations globally. We assess that over the past year, the group compromised at least 70 organizations across 37 countries, as shown in Figure 3. The attackers were able to maintain access to several of the impacted entities for months.

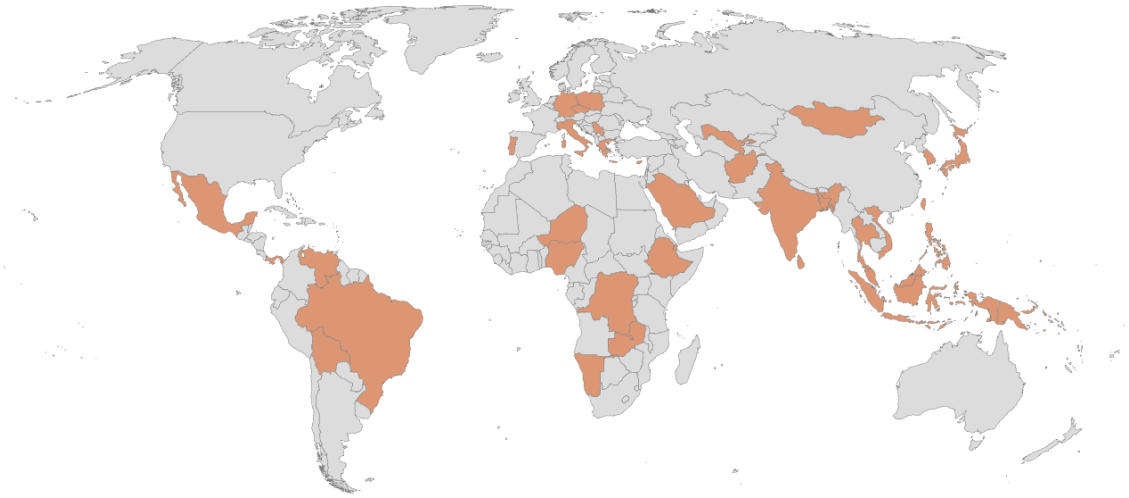

Figure 3. Locations of organizations impacted in 2025.

Impacted organizations include ministries and departments of interior, foreign affairs, finance, trade, economy, immigration, mining, justice and energy.

This group compromised one nation's parliament and a senior elected official of another. It also compromised national-level telecommunications companies and several national police and counter-terrorism organizations.

While this group might be pursuing espionage objectives, its methods, targets and scale of operations are alarming, with potential long-term consequences for national security and key services.

By closely monitoring the timing of the group's operations, we have drawn correlations between several of its campaigns and real-world events. These correlations inform assessments as to the group's potential motivations. The following sections provide additional insights from notable situations by geographic region.

## Americas

During the U.S. government shutdown that began in October 2025, the group began to display greater interest in organizations and events occurring across North, Central and South American countries. Over that month, we observed scanning of government infrastructure across Brazil, Canada, Dominican Republic, Guatemala, Honduras, Jamaica, Mexico, Panama and Trinidad and Tobago.

Perhaps the most pronounced reconnaissance occurred on Oct. 31, 2025, when we observed connections to at least 200 IP addresses hosting Government of Honduras infrastructure. The timing of this activity falls just 30 days prior to the national election, in which both candidates signaled openness to restoring diplomatic relations with Taiwan.

In addition to reconnaissance activities, we assess that the group likely compromised government entities across Bolivia, Brazil, Mexico, Panama, and Venezuela, as noted in Figure 4.

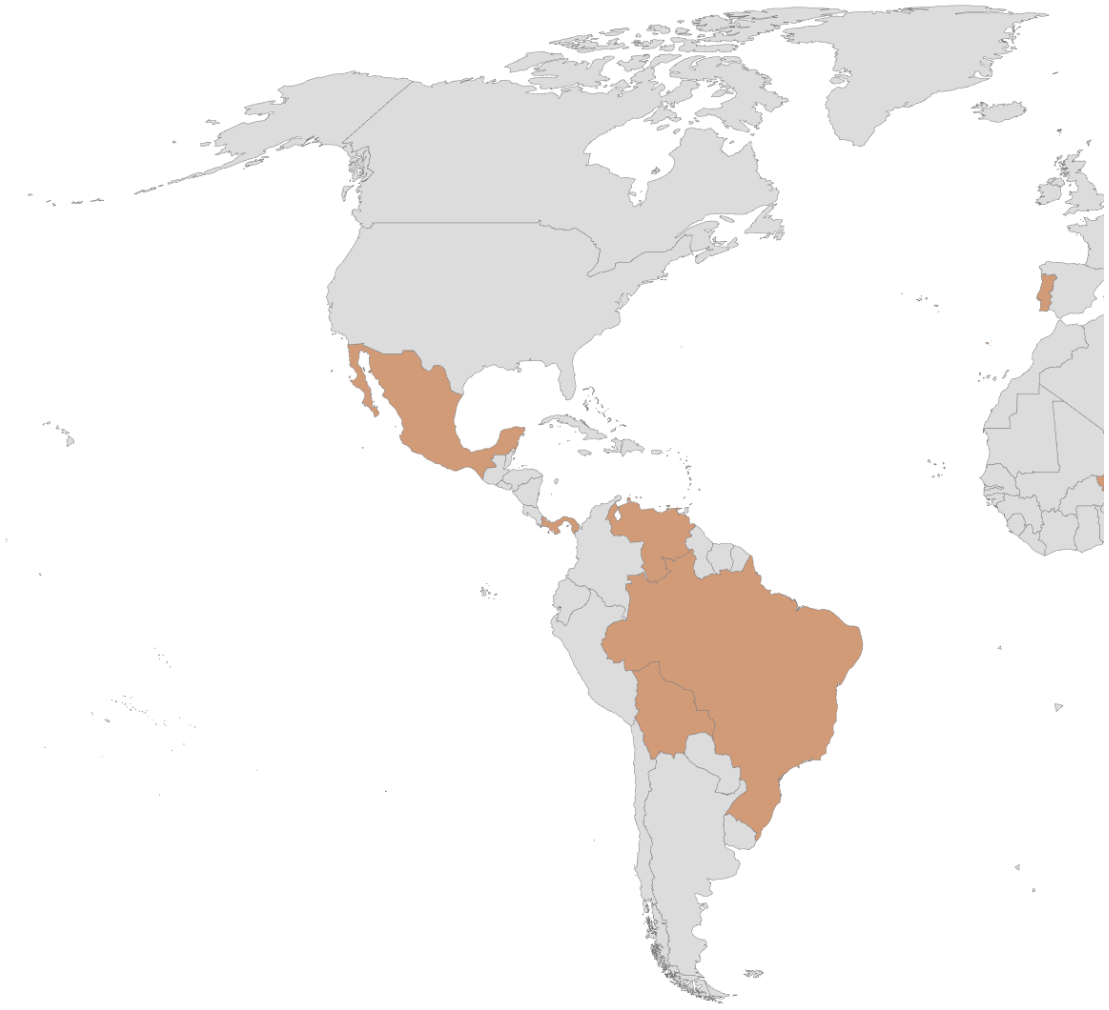

Figure 4. Location of impacted entities in the Americas.

**Bolivia**

We assess that the group likely compromised the network of a Bolivian entity associated with mining. The motivation behind this activity could be associated with interest in rare earth minerals.

We find it noteworthy that the topic of mining rights became a central focus in Bolivia's recent presidential election. In late July 2025, candidate Jorge Quiroga pledged to scrap multi-billion-dollar mining deals that the Bolivian government had previously signed with two nations.

**Brazil**

We assess that the group compromised Brazil's Ministry of Mines and Energy. Brazil is considered to have the second largest supply of rare earth mineral reserves in the world.

According to public reporting, exports of these minerals tripled in the first half of 2025. As Asian companies tighten their global control on these resources, the U.S. has begun looking to Brazil for alternative sourcing.

In October, the U.S. Charge d'Affaires in Brazil held meetings with mining executives in the country. In early November, the U.S. International Development Finance Corporation invested $465 million in Serra Verde (a Brazilian rare earth producer). This has been seen as an effort to reduce reliance on Asia for these key minerals.

**Mexico**

We assess that the group compromised two of Mexico's ministries. This activity is very likely associated with international trade agreements.

On Sept. 25, 2025, Mexico News Daily reported on an investigation into Mexico's latest plans to impose tariffs on certain goods. Coincidentally, malicious network traffic was first seen originating from networks belonging to Mexico's ministries within 24 hours of the trade probe announcement.

**Panama**

In December 2025, a report stated that local authorities destroyed a monument, prompting immediate condemnation from some leaders and calls for investigation.

Coincidentally, around the same time, we assess that TGR-STA-1030 likely compromised government infrastructure that may be associated with the investigation.

**Venezuela**

On Jan. 3, 2026, the U.S. launched Operation Absolute Resolve. This operation resulted in the capture of the Venezuelan president and his wife. In the days that followed, TGR-STA-1030 conducted extensive reconnaissance activities targeting at least 140 government-owned IP addresses.

We further assess that as early as Jan. 4, 2026, the group likely compromised an IP address that geolocates to a Venezolana de Industria Tecnológica facility, as seen in Figure 5. This organization was originally founded as a joint venture between the Venezuelan government and an Asian technology company. The venture enabled the production of computers as an early step toward deepening technology and economic ties between the two regions.


Figure 5. Geolocation data for the compromised IP address.

## Europe

Throughout 2025, TGR-STA-1030 increased its focus on European nations. In July 2025, it applied a concerted focus toward Germany, where it initiated connections to over 490 IP addresses hosting government infrastructure.

In August 2025, Czech President Petr Pavel privately met with the Dalai Lama during a trip to India. In the weeks that followed, we observed scanning of Czech government infrastructure, including:

- The Army
- Police
- Parliament
- Ministries of Interior, Finance and Foreign Affairs

In early November, a Tibetan news source announced that the Czech president would also co-patronize the Dalai Lama's 90th birthday gala. Shortly after, we witnessed a second round of scanning focused narrowly on the Czech president's website.

Separately, in late August, the group applied a concerted focus on European Union infrastructure. We observed the group attempting to connect to over 600 IP addresses hosting *.europa[.]eu domains.

In addition to reconnaissance activities, we assess that the group likely compromised government entities in countries across Cyprus, Czechia, Germany, Greece, Italy, Poland, Portugal and Serbia, as shown in Figure 6. In doing so, the group compromised at least one ministry of finance where it sought to collect intelligence on international development from both the impacted country as well as the European Union.

Figure 6. Location of impacted entities in Europe.

### Cyprus

We assess that the group compromised government infrastructure in early 2025. The timing of this activity coincided with efforts by an Asian nation to expand certain economic partnerships across Europe. At the time, Cyprus was also taking preparatory steps toward assuming the presidency of the Council of the European Union at the end of the year, a position that it currently holds.

### Greece

We assess that the group likely compromised infrastructure associated with the Syzefxis Project. This project was intended to modernize Greek public sector organizations using high-speed internet services.

## Asia and Oceania

While the group performs scanning widely across both continents, TGR-STA-1030 appears to prioritize its reconnaissance efforts against countries in the South China Sea and Gulf of Thailand regions. We routinely observe scanning of government infrastructure across Indonesia, Thailand and Vietnam. For example, in early November 2025, we observed connections to 31 IP addresses hosting Thai government infrastructure.

Additionally, it’s worth noting that the group's reconnaissance efforts often extend beyond connections to web-facing content on ports 80 and 443. In November 2025, we also observed the group attempting to initiate connections to port 22 (SSH) on infrastructure belonging to:

- Australia’s Treasury Department
- Afghanistan’s Ministry of Finance
- Nepal’s Office of the Prime Minister and Council of Ministers

In addition to reconnaissance activities, we assess that the group likely compromised government and critical infrastructure entities in countries including Afghanistan, Bangladesh, India, Indonesia, Japan, Malaysia, Mongolia, Papua New Guinea, Saudi Arabia, Sri Lanka, South Korea, Taiwan, Thailand, Uzbekistan and Vietnam, as shown in Figure 7.

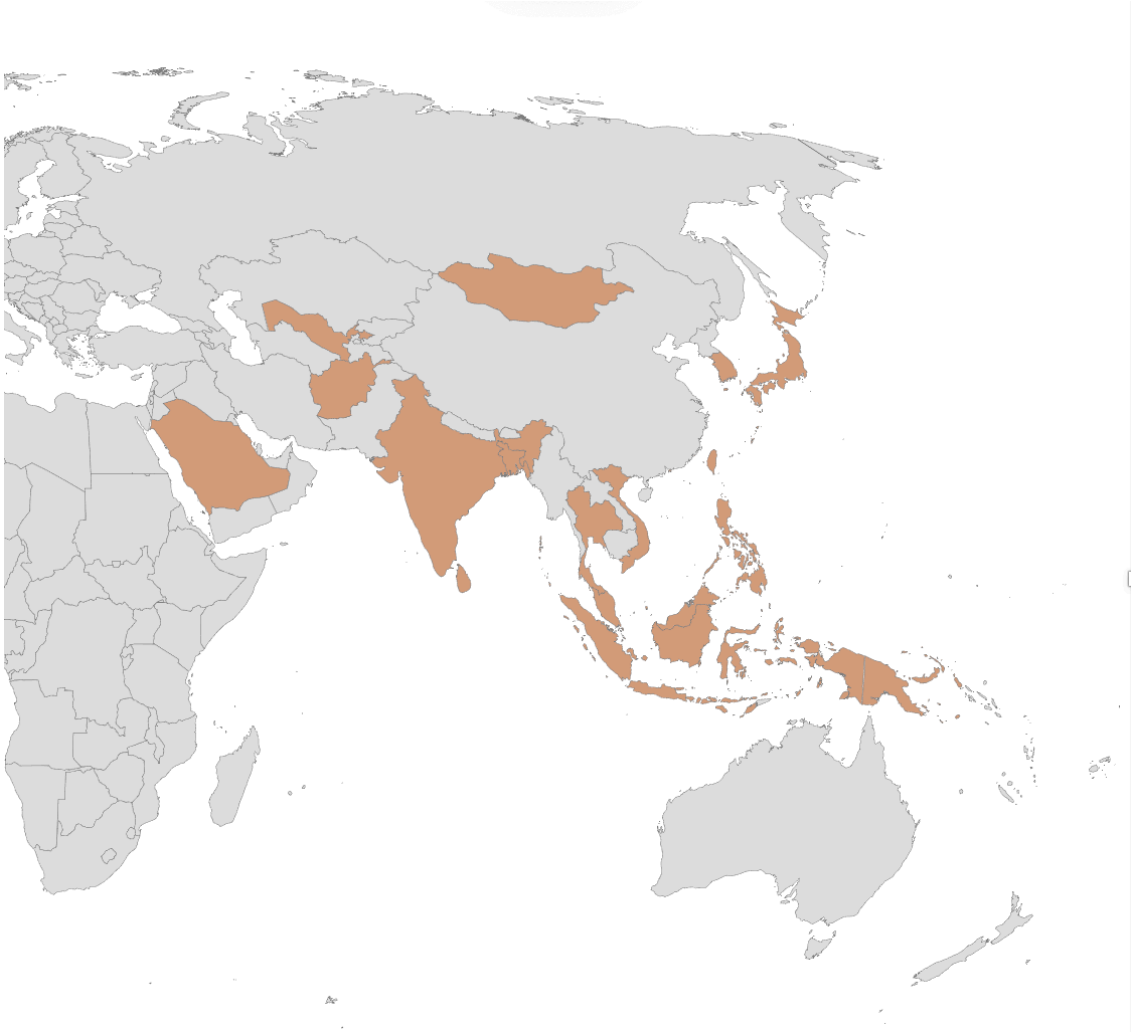

Figure 7. Location of impacted entities in Asia and Oceania.

**Indonesia**

In March 2024, Indonesia pledged to increase certain counterterrorism coordination efforts. In mid-2025, the group compromised an Indonesian law enforcement entity.

We assess that the group also compromised infrastructure associated with an Indonesian government official. This activity might have been associated with the extraction of natural resources from Papua province. We found that the official was tasked with overseeing development in the province and foreign investment in the mining sector.

The group also compromised an Indonesian airline. The compromised infrastructure geolocates to facilities at Soekarno-Hatta International Airport as shown in Figure 8. The airline had been in talks with a U.S. aerospace manufacturer to purchase new aircraft as part of its strategic growth plans. At the same time, a competing interest was actively promoting aircraft from a manufacturer based in Southeast Asia.

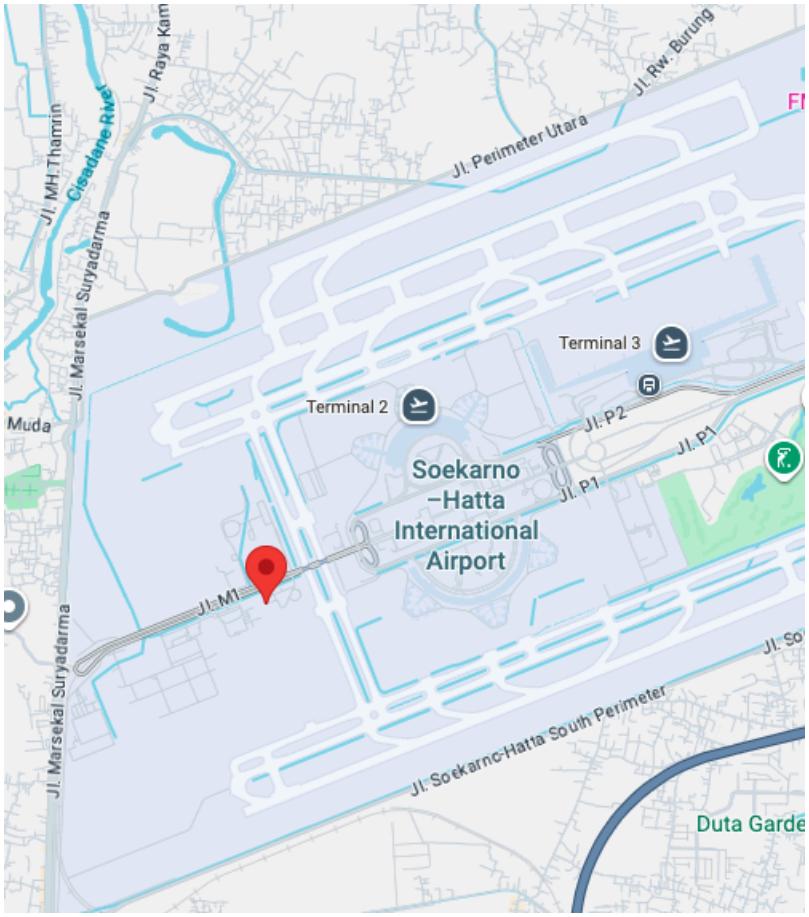


Figure 8. Geolocation data for the compromised IP address.

**Malaysia**

We assess that the group compromised multiple Malaysian government departments and ministries. Using this access, the group sought to extract immigration and economic intelligence data.

Additionally, we assess that the group compromised a large private financial entity in Malaysia that provides microloans in support of low-income households and small businesses.

**Mongolia**

The group compromised a Mongolian law enforcement entity on Sept. 15, 2025. Shortly after, Mongolia's Minister of Justice and Internal Affairs met with a counterpart from an Asian nation. Following the meeting, both countries signaled an intent to expand cooperation to combat transnational crime.

Given the timing, we assess that this activity was likely associated with intelligence gathering in support of the initial meeting and ongoing cooperation discussions.

**Taiwan**

In early 2025, the group compromised a major supplier in Taiwan's power equipment industry. With this access, we believe the group was able to access business files and directories pertaining to power generation projects

across Taiwan. We further assess that in mid-December 2025, the group regained access to this network.

### Thailand

We assess that on Nov. 5, 2025, the group compromised a Thai government department where it likely sought economic and international trade intelligence. The timing of this activity overlaps with the government's effort to expand diplomatic relations with neighboring nations. As such, we assess the activity was likely intelligence gathering in support of the visit and future cooperation discussions.

## Africa

It is our observation that when it comes to African nations, the group's focus remains split between military interests and the advancement of economic interests, specifically mining efforts.

We assess that the group likely compromised government and critical infrastructure entities in countries across the Democratic Republic of the Congo, Djibouti, Ethiopia, Namibia, Niger, Nigeria and Zambia, as shown in Figure 9:

Figure 9. Location of impacted entities in Africa.

**Democratic Republic of the Congo (DRC)**

We assess that in December 2025, the group compromised a government ministry in this country. We found that earlier in the year, an Asian mining firm was responsible for an acid spill that caused significant impacts to a river in neighboring Zambia. In November 2025, a second spill by another Asian company impacted the waterways around Lubumbashi, the second-largest city in the DRC. This event prompted authorities to suspend mining operations for a subsidiary of the Zhejiang Huayou Cobalt Co. Given the timing and the group's unique focus on mining operations, we assess that activity could be related to this mining situation.

**Djibouti**

Several nations maintain military bases in Djibouti. These bases enable combating piracy on the high seas as well as other regional logistics and defense functions across the Arabian Sea, Persian Gulf and Indian Ocean.

In mid-November, a new Naval Escort Group from one of the nations assumed responsibilities in the region. During its operational debut, the group escorted a Panamanian-registered bulk carrier called the Nasco Gem that carries cargo such as coal and ore. In the context of cyber activity, this could be related to the targeting of mining sectors we observed from TGR-STA-1030.

We assess that in late October 2025, the group gained access to a Djibouti government network. Given the timing of the activity, we believe it might be associated with intelligence collection in support of the naval handover operations.

**Zambia**

We assess that the group compromised a Zambian government network in 2025. This activity is likely associated with the Sino-Metals Leach Zambia situation.

In February, a dam that held waste from an Asian mining operation collapsed and polluted a major river with cyanide and arsenic. The situation and associated clean-up efforts remain a political point of contention.

## Conclusion

TGR-STA-1030 remains an active threat to government and critical infrastructure worldwide. The group primarily targets government ministries and departments for espionage purposes. We assess that it prioritizes efforts against countries that have established or are exploring certain economic partnerships.

Over the past year, this group has compromised government and critical infrastructure organizations across 37 countries. Given the scale of compromise and the significance of the impacted government entities, we are working with industry peers and government partners to raise awareness of the threat and disrupt this activity.

We encourage network defenders and security researchers to leverage the indicators of compromise (IoCs) provided below to investigate and deploy defenses against this group.

### Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through the following products and services:

- Advanced URL Filtering and Advanced DNS Security identify known URLs and domains associated with this activity as malicious.
- The Advanced WildFire machine-learning models and analysis techniques have been reviewed and updated in light of the indicators shared in this research.
- Advanced Threat Prevention is designed to defend networks against both commodity threats and targeted threats.
- Cortex XDR and XSIAM help to protect against the threats described in this blog, by employing the Malware Prevention Engine. This approach combines several layers of protection, including Advanced WildFire, Behavioral Threat Protection and the Local Analysis module, designed to prevent both known and unknown malware from causing harm to endpoints.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 000 800 050 45107
- South Korea: +82.080.467.8774

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

## Indicators of Compromise

### IP Addresses

- 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

### 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

### Phishing/Downloader SHA256

- 66ec547b97072828534d43022d766e06c17fc1cafe47fbd9d1ffc22e2d52a9c0
- 23ee251df3f9c46661b33061035e9f6291894ebe070497ff9365d6ef2966f7fe

### Cobalt Strike SHA256

- 5175b1720fe3bc568f7857b72b960260ad3982f41366ce3372c04424396df6fe
- 358ca77ccc4a979ed3337aad3a8ff7228da8246eebc69e64189f930b325daf6a
- 293821e049387d48397454d39233a5a67d0ae06d59b7e5474e8ae557b0fc5b06
- c876e6c074333d700adf6b4397d9303860de17b01baa27c0fa5135e2692d3d6f
- b2a6c8382ec37ef15637578c6695cb35138ceab42ce4629b025fa4f04015eaf2
- 5ddeff4028ec407ffdaa6c503dd4f82fa294799d284b986e1f4181f49d18c9f3
- 182a427cc9ec22ed22438126a48f1a6cd84bf90fddb6517973bcb0bac58c4231

### ShadowGuard SHA256

- 7808b1e01ea790548b472026ac783c73a033bb90bbe548bf3006abfbcb48c52d

### CVE-2019-11580 Exploit SHA256

- 9ed487498235f289a960a5cc794fa0ad0f9ef5c074860fea650e88c525da0ab4

*Updated Feb. 5, 2026, at 7:40 a.m. PT to add Cortex product protections language.*

---

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