TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies | Recorded Future

By Insikt Group®

Archived: 2026-04-02 10:43:26 UTC

Summary

Recorded Future's Insikt Group identified a suspected cyber-espionage campaign by TAG-100, targeting global government and private sector organizations. TAG-100 exploited internet-facing devices and used open-source tools like the Go backdoor Pantegana. The campaign compromised two Asia-Pacific intergovernmental organizations and targeted multiple diplomatic and trade entities.

TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies

TAG-100 employs open-source remote access capabilities and exploits various internet-facing devices to gain initial access. This activity highlights the increasing trend of cyber-espionage using open-source tools, making it easier for less capable threat actors and reducing the need for customized capabilities. Two major Asia-Pacific intergovernmental organizations, along with multiple diplomatic, trade, and private sector entities globally, were likely compromised by TAG-100.

Key Findings

- TAG-100 has compromised organizations in at least ten countries across Africa, Asia, North America, South America, and Oceania.
- The group used open-source Go backdoors Pantegana and SparkRAT post-exploitation.
- TAG-100 targeted various internet-facing products, including Citrix NetScaler, F5 BIG-IP, Zimbra, Microsoft Exchange, SonicWall, Cisco ASA, Palo Alto Networks GlobalProtect, and Fortinet FortiGate.
- Following the release of a PoC exploit for Palo Alto Networks GlobalProtect firewall vulnerability CVE-2024-3400, TAG-100 conducted reconnaissance and attempted exploitation against dozens of US-based organizations.

Impact and Implications

The exploitation of vulnerable internet-facing devices by TAG-100 is particularly concerning due to the limited visibility and logging capabilities of these devices. This reduces the risk of detection post-exploitation and exposes

organizations to operational downtime, reputational damage, and regulatory fines. The use of open-source tools also allows state-sponsored threat actors to outsource cyber operations to less capable groups, increasing the intensity and frequency of attacks on enterprise networks.

Mitigations

Organizations should:

- Configure intrusion detection and prevention systems to alert on and block suspicious IP addresses and domains.
- Ensure security monitoring for all external-facing services and devices.
- Prioritize patching vulnerabilities, especially those exploited in the wild.
- Implement network segmentation and multi-factor authentication.
- Use the Recorded Future® Threat Intelligence module to detect and block malicious infrastructures like Pantegana, SparkRAT, and Cobalt Strike command-and-control (C2) servers in real-time.
- The Recorded Future® Third-Party Intelligence module helps monitor real-time outputs to identify suspected intrusion activities involving key vendors and partners.
- Monitoring Malicious Traffic Analysis (MTA) enables Recorded Future clients to proactively alert and monitor infrastructure involved in communication with known TAG-100 C2 IP addresses.

Outlook

TAG-100's activities highlight a persistent threat to internet-facing devices, with both financially motivated and state-sponsored threat actors likely to continue exploiting these vulnerabilities. The US and UK governments are working to improve security, but vulnerable network edges remain a significant risk. Financially motivated and state-sponsored threat actors will likely continue exploiting these vulnerabilities.

To read the entire analysis, click here to download the report as a PDF.
