ADVISORY FOR ICM SECTOR

PHANTOM PANDA compromise of Southeast Asian Telecom

Original report published on: July 15, 2026

Executive Summary

On 1 July 2026, CrowdStrike discovered that PHANTOM PANDA (also known as GALLIUM, Granite Typhoon) had compromised a Java web server belonging to a Southeast Asia-based telecommunications operator. The Threat Actor (TA) deployed a likely SoftEther VPN client and conducted extensive hands-on-keyboard activity. This included host and network reconnaissance, credential harvesting and enumeration of internal SMS infrastructure. The TA also attempted to download tools from compromised third-party infrastructure, a tactic that PHANTOM PANDA had newly adopted. This campaign is attributed to PHANTOM PANDA with moderate confidence.

Background

PHANTOM PANDA had been known to exploit public-facing applications, such as web servers, use dynamic DNS services to register command-and-control (C2) domains, and use Mimikatz to harvest credentials and exfiltrate Active Directory data. Historically, the group had targeted organisations in the telecommunications, technology, and government sectors.

The TA deployed a likely SoftEther VPN client to establish persistent access. They conducted host and network reconnaissance using *cat /etc/hosts*, *ls -anl /*, *netstat -an | grep EST* and *FScan* from /var/tmp, then used *ping* and *curl* to connect to their C2 domain (censysio[.]softether[.]net) and IP address (38[.]60 [.]250[.]40 over TCP port 443 and UDP ports 53, 15581, and 40002). Both nodes had previously been used in suspected TA activity against multiple telecommunications entities between December 2024 and late 2025.

Post reconnaissance, PHANTOM PANDA used *curl* to make requests to an unmanaged internal host likely related to mobile SMS communications. The TA accessed /etc/passwd, likely for credential harvesting, and attempted to authenticate to the entity's Outlook Web Access mail service. They attempted to download web shells, including Godzilla, from likely compromised infrastructure associated with an agricultural-sector victim. The TA subsequently attempted to connect to systems associated with an automotive-sector victim, likely to obtain additional tools. However, no successful downloads were observed.

Based on shared C2 infrastructure, overlapping TTPs, and the deployment of a likely SoftEther VPN client, the activity was attributed to PHANTOM PANDA with moderate confidence. However, this intrusion lacked other known techniques used by this TA.

Detection and Mitigation

IMDA recommends that organisations perform continual testing and validation of existing security controls to ensure detection and prevention of PHANTOM PANDA-related activities identified in this advisory:

- Scan for Indicators of Compromise (Annex A) to detect threat activities in your environment.
- Refer to the MITRE ATT&CK techniques (Annex B) in this advisory to:
  - Create, test and validate detection rules against the threat behaviours.
  - Validate and deny or disable processes, ports and protocols that have no legitimate business need.
- Patch internet-facing web servers, VPN appliances and other exposed devices with the latest vendor-supported security updates, after risk and impact assessment.
- Restrict external-facing services on internet-accessible servers to only those required for business operations.
- Deploy Endpoint Detection and Response (EDR) on internet-facing and internal servers to detect and block suspicious commands; FScan, C2 connections using curl or ping, and processes executed from /var/tmp.
- Deploy Network Detection and Response (NDR) to identify possible C2 activity by detecting periodic beaconing, anomalous outbound connections and unusual traffic from web servers and VPN devices; investigate high outbound-data volumes over these channels as potential data exfiltration.
- Enforce controlled software deployment through approved software repositories and application whitelisting, then periodically run vendor-provided file-integrity checks against binaries and configuration files.
- Regular monitoring of new local and privileged account creation on servers, security products and management systems, especially if they are internet-facing and validate them against approved access request.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

Type	Value	Comment
IP	38[.]60[.]250 [.]40	C2 IP Address

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Remarks
Resource Development	T1584 – Compromise Infrastructure	PHANTOM PANDA leverages compromised third-party infrastructure in its operations.
Initial Access	T1190 – Exploit Public-Facing Application	PHANTOM PANDA exploited a Java web server.
Discovery	T1016.001 – System Network Configuration Discovery: Internet Connection Discovery	PHANTOM PANDA used ping and curl commands to test access to public hosts and adversary-controlled infrastructure.

Command and Control	T1219 – Remote Access Tools	PHANTOM PANDA likely deployed a SoftEther VPN Client.