ADVISORY FOR ICM SECTOR

Phantom Taurus targets telecom for cyber espionage

Original report published on: September 30, 2025[1]

Executive Summary

Palo Alto Networks Unit 42 published a multi-year investigation into Phantom Taurus (CL-STA-0043, TGR-STA-0043), a threat actor that conducts long-term espionage campaigns against government and telecom organisations in the Middle East, Africa, and Asia.

Researchers observed that the group's operations have shifted over time from exfiltrating data from email servers to directly targeting SQL databases and internet-facing IIS web servers. Phantom Taurus deploys NET-STAR, a web-based, fileless .NET malware suite on IIS web servers which is capable of in-memory execution, bypassing Anti-Malware Scan Interface (AMSI) and Event Tracing for Windows (ETW), and using time-stomping to evade detection. The group also executes *mssq.bat* scripts, executed via WMI with stolen credentials to query SQL databases and exfiltrate sensitive records.

Background

Phantom Taurus focuses on collecting sensitive, non-public information from high-value organisations. Their recent operations include:

- Remote SQL database access using *mssq.bat* and WMI with stolen credentials
- Dynamic query execution to extract region-specific data (e.g., Afghanistan, Pakistan)
- Deployment of NET-STAR backdoors targeting IIS web servers for stealthy IIS server compromise:
    - IIServerCore – modular, fileless backdoor running entirely in memory
    - AssemblyExecuter V1 – executes .NET payloads in memory
    - AssemblyExecuter V2 – enhanced version with advanced evasion including AMSI and ETW bypass
- Use of encrypted C2 channels for command execution and data exfiltration

This reflects a clear evolution from email-centric espionage to structured data collection and sophisticated web server exploitation.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention of the NET-STAR malware identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Patch and secure internet-facing systems, especially IIS web servers, ensuring all critical updates and secure configurations are applied.
- Deploy tools such as EDR to detect in-memory execution and fileless malware beyond traditional antivirus.
- Monitor SQL Server activity for new queries, high-privileged account use, and restrict execution rights for scripts such as *mssq.bat*.

- Implement Data Loss Prevention (DLP) solutions to ensure sensitive data stays within approved networks and to block unauthorised cloud storage access.
- Monitor egress traffic for unexpected geolocation or exceeding a size threshold, indicating possible data exfiltration.

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

SHA256 Hash	Description
eeed5530fa1cdeb69398dc058aaa01160eab15d4dcdcd6cb841240987db284dc	ServerCore.dll
3e55bf8ecaeec65871e6fca4cb2d4ff2586f83a20c12977858348492d2d0dec4	ExecuteAssembly.dll
afcb6289a4ef48bf23bab16c0266f765fab8353d5e1b673bd6e39b315f83676e	ExecuteAssembly.dll
b76e243cf1886bd0e2357cbc7e1d2812c2c0ecc5068e61d681e0d5cff5b8e038	ExecuteAssembly.dll

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Persistence	T1505.003	Server Software Component: Web Shell
	T1505.001	Server Software Component: SQL Stored Procedures
Defence Evasion	T1070.006	Indicator Removal: Time-Stomp
	T1620	Reflective Code Loading
	T1055	Process Injection
Collection	T1114.002	Email Collection: Remote Email Collection
Exfiltration	T1567	Exfiltration Over Web Service

References

1. ^ “Phantom Taurus: A New Chinese Nexus APT and the Discovery of the NET-STAR Malware Suite”