مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

# Tropic Trooper APT Group Targeting Middle East Government Entities

Tracking #:432316304

Date:18-09-2024



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers detected a sophisticated cyber espionage campaign targeting a government entity in the Middle East, attributed with high confidence to the Chinese-speaking APT group known as Tropic Trooper.

## TECHNICAL DETAILS:

Tropic Trooper has been active since 2011, primarily targeting sectors such as government, healthcare, transportation, and high-tech industries in regions including Taiwan, the Philippines, Hong Kong, and now the Middle East. Their recent campaigns have shown a strategic shift towards targeting entities involved in human rights studies. In 2024, the APT group known as Tropic Trooper (also referred to as KeyBoy and Pirate Panda) has intensified its cyber espionage activities, particularly targeting government entities in the Middle East.

In June 2024, telemetry alerts indicated the presence of a new variant of the China Chopper web shell on a compromised public server running Umbraco CMS. This web shell was used to execute commands remotely and drop additional malware components.

- Malware Clusters: The investigation revealed multiple malware families deployed during the attack:
- Web Shells: Variants of .NET web shells were found that allowed attackers to maintain remote access.
- Post-Exploitation Tools: Tools such as Fscan and Swor were identified for network scanning and lateral movement within the victim's network.
- DLL Search-Order Hijacking: New variants of malware utilized DLL search-order hijacking techniques to load malicious code through legitimate executables.
- Attack Vector: The attackers exploited known vulnerabilities in Microsoft Exchange and Adobe ColdFusion to deploy their payloads. The use of unpatched software significantly increased the risk of successful exploitation.

## INDICATORS OF COMPROMISE:

Attached File

## RECOMMENDATIONS:

- Identify and analyse all IOCs associated with the Tropic Trooper campaign, including file hashes, IP addresses, and domain names linked to the observed malware and web shell activities.
- Implement blocking measures for the identified malicious IOCs.
- Immediate Security Assessment: Conduct a thorough assessment of all web applications, particularly those using content management systems like Umbraco, to identify and remediate any unpatched vulnerabilities.
- Implement Web Application Firewalls (WAF): Deploy WAFs to monitor and filter incoming traffic to web applications, providing an additional layer of defense against web shell attacks.

- Regular Software Updates: Ensure that all software, especially CMS platforms and their plugins, are regularly updated to mitigate risks associated with known vulnerabilities.
- Intrusion Detection Systems (IDS): Utilize IDS to detect suspicious activities and potential breaches in real-time, enabling rapid response to threats.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:


- https://securelist.com/new-tropic-trooper-web-shell-infection/113737/?reseller=gl_regular-sm_acq_ona_smm__onl_b2b_twi_lnk_sm-team_____f914262e964e2827&utm_source=twitter&utm_medium=social&utm_campaign=gl_regular-sm_ab0218&utm_content=link&utm_term=gl_twitter_organic_27e218ehlldj4hr&kaspr=2aex