Article

Oct 2024

Tropic Trooper spies on government entities in the Middle East

An Advanced Persistent Threat group, Tropic Trooper, launched an attack against a middle eastern government entity – although thought to have started in June 2023, it was only discovered in August of 2024.An Advanced Persistent Threat group, Tropic Trooper, launched an attack against a middle eastern government entity – although thought to have started in June 2023, it was only discovered in August of 2024.

Andrea Malortigue
Information Security Consultant
Email andrea.malortigue@Waterstons.com

The government entity published content focused on human rights and the Israel-Palestine conflict.

The malicious actors used an unpatched vulnerability to create a web shell, China Chopper, on the public facing server used for content management. The web shell was then used to upload several exploitation tools to pursue the attack, including reconnaissance, and obscuring open-source tools that are maintained by Chinese-speaking developers. The attackers then attempted to create a backdoor by compromising legitimate files to remain undetected, which was blocked at first by the antivirus present on the targeted server. The hackers then modified their program to bypass detection.

The attack was only detected when a new variant of the China Chopper web shell was detected on the public-facing server.

Wider context

The sophistication behind this incident highlights the growing interest of Chinese state-sponsored threat actors for the middle eastern region. Tropic Trooper, which is thought to be behind the attack has historically been targeting public and private sector entities in Taiwan, the Philippines, and Hong Kong.

The aim of such attack seems to focus on political cyber espionage, which confirms the middle east as an area of critical interest for powers all around the world.

Recommendations

Ensure all systems, especially third-party and external-facing applications, are regularly updated to patch known vulnerabilities.

Implement 24x7 monitoring solutions to detect unusual activities, such as the deployment of web shells.

Have signature-based antivirus that is fed from threat intelligence to stay up to date with the newest trends and tools.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430