APT41's Unprecedented Operations in Africa: A Strategic Expansion

Infosources™

July 23, 2025

China-linked threat actor APT41 has expanded its operations into a new and unexpected theatre: Africa. Long associated with state-backed cyber-espionage and financially motivated attacks across Asia, Europe, and North America, the group has now been observed targeting an African government IT provider with a tailored malware campaign. This shift signals a potential new strategic direction for APT41, raising fresh concerns about China's cyber posture on the continent and the vulnerability of emerging digital infrastructures across Africa.

APT41's sudden appearance in Africa isn't just surprising — it's strategic. This is a group long known for high-value espionage operations linked to Chinese state interests, typically focusing on targets in Taiwan, the U.S., or sectors like healthcare, education, and telecoms in Europe and Asia. Africa, until now, barely registered on their radar. That's changed.

In what looks like a calculated shift, APT41 went after an African government IT service provider. Kaspersky uncovered the activity after detecting suspicious signals from several workstations within the victim organization. No names have been disclosed, but the tactics were unmistakable. The group didn't just deploy generic malware — they embedded malware laced with internal IP addresses, proxy configurations, and infrastructure specifics. That suggests deep reconnaissance, possibly insider knowledge. One of their command-and-control nodes? A SharePoint server inside the victim's own network. That's not opportunistic targeting — that's bespoke malware engineering.

The technical footprint bore all the hallmarks of APT41's playbook. Initial access was gained via **Impacket**, with the **WmiExec** and **Atexec** modules helping them identify and stay rooted in the environment. From there, they rolled out **Cobalt Strike** to maintain persistence and coordinate the next phases. Data and credential theft came next, using **Mimikatz** to extract secrets, **Pillager** for broader data harvesting, and **RawCopy** to extract files without triggering alarms. For remote access, **Neo-reGeorg** served as a backdoor through a hijacked web server.

APT41 doesn't just reuse tools — they evolve with the network. During the operation, they adjusted tactics on the fly, recompiling executables into DLLs to sideload them silently. They used internal services for communication and data exfiltration, making traffic blend in with legitimate operations. This level of operational maturity makes them hard to track and harder to stop mid-operation.

Why Africa now? It's not just a soft target. The region's digital expansion has outpaced its cybersecurity investments. INTERPOL recently flagged a massive uptick in cybercrime across the continent — online scams are exploding, and digital infrastructures are increasingly under strain. In that context, APT41's move may be less about the specific victim and more about footholds. This could be early-stage reconnaissance for long-term strategic positioning.

Whether this is a one-off or a sign of a broader campaign remains to be seen. But one thing is clear: APT41 is adapting, expanding, and exploiting new terrain — and Africa's networks are now very much on their map.

💡

APT41 *(a.k.a. Wicked Panda, Barium, Brass Typhoon, Winnti) represents a decentralized constellation of Chinese cyber subgroups operating under varied aliases. The threat actor demonstrates a dual-function model—conducting both* ***state-sponsored espionage*** *and* ***financially motivated cybercrime****. The group is widely believed to operate with the tacit or direct backing of China's* ***Ministry of State Security (MSS)****. Active since* ***at***

least 2012*, APT41 has evolved into one of the most persistent Chinese threat collectives. Their operations span a wide toolkit: credential theft, exploitation of known and zero-day vulnerabilities, deployment of ransomware payloads, and cryptojacking malware. This multi-pronged approach enables both intelligence collection and profit generation.*

In 2020, the U.S. Department of Justice formally indicted five individuals tied to APT41, linking them to a long-running campaign involving the compromise of over 100 organizations worldwide. Victims included entities in healthcare, telecommunications, higher education, and software development, with operations extending well beyond U.S. borders.

APT41 exemplifies China's hybrid cyber strategy—blurring lines between state interest and individual enrichment. The actor's broad targeting scope and proven capacity to evade detection reinforce its high-risk designation by Western intelligence agencies.