BackdoorDiplomacy Wields New Tools in Fresh Middle East Campaign

By Adrian SCHIPOR

Archived: 2026-04-05 14:10:06 UTC

Bitdefender researchers have uncovered a new cyber-espionage campaign targeting a telecommunications firm in the Middle East. While investigating a set of binaries vulnerable to sideloading attacks, we identified a cyber-espionage operation most likely carried out by Chinese threat actor BackdoorDiplomacy.

Who is BackdoorDiplomacy?

APT group BackdoorDiplomacy, which has been operating at least since 2017, is known for its attacks against institutions in the Middle East and Africa as well as in the United States.

This report covers another campaign against a telecom company in the Middle East. It also documents a set of new tools the group adopted in 2022.

Attack at a glance

- The infection vector pointed to a vulnerable Exchange server, exploiting ProxyShell. Forensic evidence shows the attack started in August 2021, when the group deployed the NPS proxy tool and IRAFAU backdoor into the organization.
- Starting in February 2022, the threat actors used another tool - Quarian backdoor, along with several other scanners and proxy/tunneling tools.
- Artifacts reveal the use of keyloggers and exfiltration tools that link this campaign to a cyber-espionage operation.

Indicators of Compromise

An up-to-date, complete list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users. Currently known indicators of compromise can be found in the whitepaper below.

Download the whitepaper

Source: https://www.bitdefender.com/blog/labs/backdoor-diplomacy-wields-new-tools-in-fresh-middle-east-campaign/