

Chinese Hackers Target Kenya's Government in Long-Term Cyber Espionage Campaign

Chinese hackers have reportedly conducted a widespread and prolonged series of cyber intrusions targeting key ministries and state institutions of the Kenyan government. According to multiple sources, cybersecurity research reports, and Reuters' analysis of technical data, the hacking campaign aimed to gain access to information about Kenya's debt owed to Beijing. Kenya's strategic position in the Belt and Road Initiative, China's global infrastructure network, makes it a crucial link in China's economic interests. China denies any involvement in the hacking activities and asserts its commitment to combating cyberattacks and theft.

The cyber intrusions, spanning three years, targeted eight ministries and government departments in Kenya, including the presidential office. According to a Reuters report, sources revealed that the attacks were primarily focused on gathering information about Kenya's debt situation. China's extensive lending to African countries, including Kenya, for infrastructure projects has made it the largest bilateral creditor to the nation. The hacking campaign demonstrates China's willingness to use espionage capabilities to protect its economic and strategic interests abroad.

The breach began in late 2019 with a spearphishing attack, where a government employee unknowingly downloaded an infected document, enabling hackers to access the network and infiltrate other agencies. Documents stolen included sensitive information from the Ministry of Foreign Affairs and the Finance Department, indicating a targeted focus on the debt situation. Chinese cyber spies conducted a persistent and prolonged hacking campaign against the president's office, defence, information, health, land, and interior ministries, as well as other institutions.



A conductor waits on a platform as an SGR (*China-built Mombasa-Nairobi Standard Gauge Railway*) train travelling from Nairobi arrives at Mombasa Terminus in Mombasa, Kenya on October 24, 2019. Baz Ratner/Reuters

Kenya's financial strains and the impact of the COVID-19 pandemic on the global economy added pressure on the country's debt burdens. Kenya managed to secure a temporary debt repayment moratorium from China. The breach of Kenya's National Intelligence Service (NIS) email server raised concerns about the hackers' intentions and potential access to information regarding Kenya's debt management.

Although the motive for the attacks and the information obtained remains unclear, the defence contractor's report suggests that China targeted the NIS to gather insights into Kenya's debt repayment strategies.

China's hacking team known as "BackdoorDiplomacy" was identified as the likely perpetrator, given its record of furthering Chinese diplomatic objectives through cyber espionage. The group has previously targeted governments and institutions in Asia and Europe.

The [report says](#), Chinese officials have denied any involvement in the hacking activities and emphasized China's commitment to cybersecurity. Cybersecurity researchers confirm that

BackdoorDiplomacy, the state-linked hacking team responsible for the attacks, operates under the sponsorship of the Chinese government. The focus and scale of the hacking activities in Kenya, particularly regarding the debt situation, highlight the group's priority.

China is Leveraging its cyber capabilities

The hacking activities demonstrate China's willingness to leverage its cyber capabilities to protect its economic and strategic interests abroad. Kenya, like other African nations, faces financial strains due to the growing cost of servicing external debt, with China being the largest bilateral creditor. China denies involvement in the hacking campaign and asserts its commitment to cybersecurity.

The breach raises concerns about the vulnerability of countries heavily reliant on Chinese loans and the potential risks associated with their debt burdens.

Subscribe to the International Relations Updates by The Kootneeti

* indicates required

Full Name

Email Address *

Subscribe

made with  mailchimp

Chinese Hackers Target Kenya's Government in Long-Term Cyber Espionage Campaign



CERTIFICATE COURSE IN INTERNATIONAL RELATIONS

SIX-WEEK ONLINE COURSE IN INTERNATIONAL RELATIONS BY THE KOOTNEETI

JOIN TODAY!

team@thekootneeti.com
courses.thekootneeti.in
(+91) 120 4565994

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team

Facebook Comments