Six Australian MPs Confirm They were Targeted by China's APT31 Hackers

⋮ 5/6/2024

Six Australian Members of the Parliament confirmed today that they were targeted by Chinese-state hackers APT31 in a brazen cyberattack whose aim was to gather intelligence on these individuals.

The Inter-Parliamentary Alliance on China whose members were victims of this hacking attempt said, "The politicians confirmed details with both the IPAC Secretariat and the Australian Government."

> *"The apparent intention [of the cyberattack] was to garner sufficient information to mount more sophisticated follow-on attacks, escalating in severity."*

Those targeted included Senator James Paterson, Senator Claire Chandler, Senator Alex Antic, David Smith MP, Daniel Mulino MP and Tim Wilson MP.

Security Agencies Chose to Remain Tight-Lipped

Australia's security agencies reportedly received two warnings about Chinese hackers targeting Australian MPs, but they chose not to inform the lawmakers about the cyberattacks.

"It is staggering that both the targeted members of parliament and the broader Australian public have been kept in the dark about a direct attempt at cyber interference against Australian parliamentarians," Senator Claire Chandler said.

> *"Incredibly, despite Australian authorities being notified of this hacking attempt in 2022, agencies did not alert my colleagues and I that we had been targeted.It's unacceptable that this information was withheld from us for two years,"* Chandler added.

The Five Eyes intelligence agency reportedly alerted Australia's security agencies in mid-2021 about attacks that occurred earlier in January. Then, in June 2022, the FBI officially notified Australian authorities about attempts by the Chinese hacking group APT31 to target six Australian MPs.

However, the agencies opted against informing the Government or the affected MPs. The IPAC, consisting of 20 Australian MPs, only became aware of the attempted attack when the US Department of Justice indicted seven Chinese hackers in April this year -three years after the initial warning.

The National Cyber Security Centre of the United Kingdom also called out the Chinese APT31 actors for their malicious cyber targeting of UK's democratic institutions and parliamentarians earlier in March.

Following this revelation, MPs demanded an explanation from the Australian Security Intelligence Organisation regarding the lack of notification. After receiving a briefing, they released a joint statement today expressing outrage and demanding a robust response to protect Australian sovereignty.

"We were not informed by Australian agencies at any time since 2021 about this targeting," the statement from IPAC members targeted by APT31 said.

> *"This was not an attack on any single party or House of Parliament. This was an attack on Australian parliamentarians from both Houses and both parties who have dared to exercise their legitimate democratic right to criticize Beijing. As such, it was an attack on Parliament as a whole and demands a robust and proportionate response,"* the IPAC members' statement said.

"It is very worrying for our democracy that elected members of parliament have been targeted by PRC-state sponsored hacking attempts specifically because we have expressed concern about the behavior of the PRC, including human rights violations in Xinjiang and coercive behavior against Australia," Senator Claire Chandler said.

"It is in Australia's national interest for Australians to be properly informed about the behavior of the PRC government. The withholding of information about the targeting of Australian elected representatives by state-affiliated cyber criminals means that Australians have been given a misleading impression of the PRCs behavior towards our country," Chandler added.

The targeted IPAC members insisted on being informed about future attempts to target them by state-sponsored groups, for which they have received an assurance from the government.

> *"I welcome the assurance that in future agencies will inform MPs about any attempts by state-sponsored cyber actors to target parliamentarians,"* Senator Claire Chandler said.

The Australian agencies likely refrained from informing MPs because they considered the attacks crude and unsuccessful, according to Austrlian news agency The Nightly. Moreover, they occurred during a period when MPs and the public were already being cautioned to enhance their cybersecurity.

Paterson, who is also the co-chair of IPAC Australia, denounced the attempted hack.

> *"Targeting parliamentarians, as the CCP has done, is not the act of a friend. It is yet another obstacle to a normal bilateral relationship. We should never hesitate to call out this behavior or be afraid to impose real costs to deter it,"* he tweeted.

APT31 Used Pixel Tracking Emails

APT31 hackers targeted MPs with pixel tracking emails from a domain pretending to be a news outlet. If opened, these emails tracked the recipients' online behavior.

According to the FBI's indictment released last month, the hackers spammed various government individuals worldwide associated with IPAC, with more than 10,000 malicious emails that also exploited zero-days and resulted in potential compromise of economic plans, intellectual property and trade secrets.

Last month, FBI Director Christopher Wray highlighted the magnitude of Chinese hacking, stating that it surpassed that of every other major nation combined. He underscored the overwhelming scale of Chinese cyber operations, indicating the challenges faced by law enforcement in countering these threats.