Indonesian intelligence agency compromised in suspected Chinese hack

therecord.media/indonesian-intelligence-agency-compromised-in-suspected-chinese-hack/

September 10, 2021

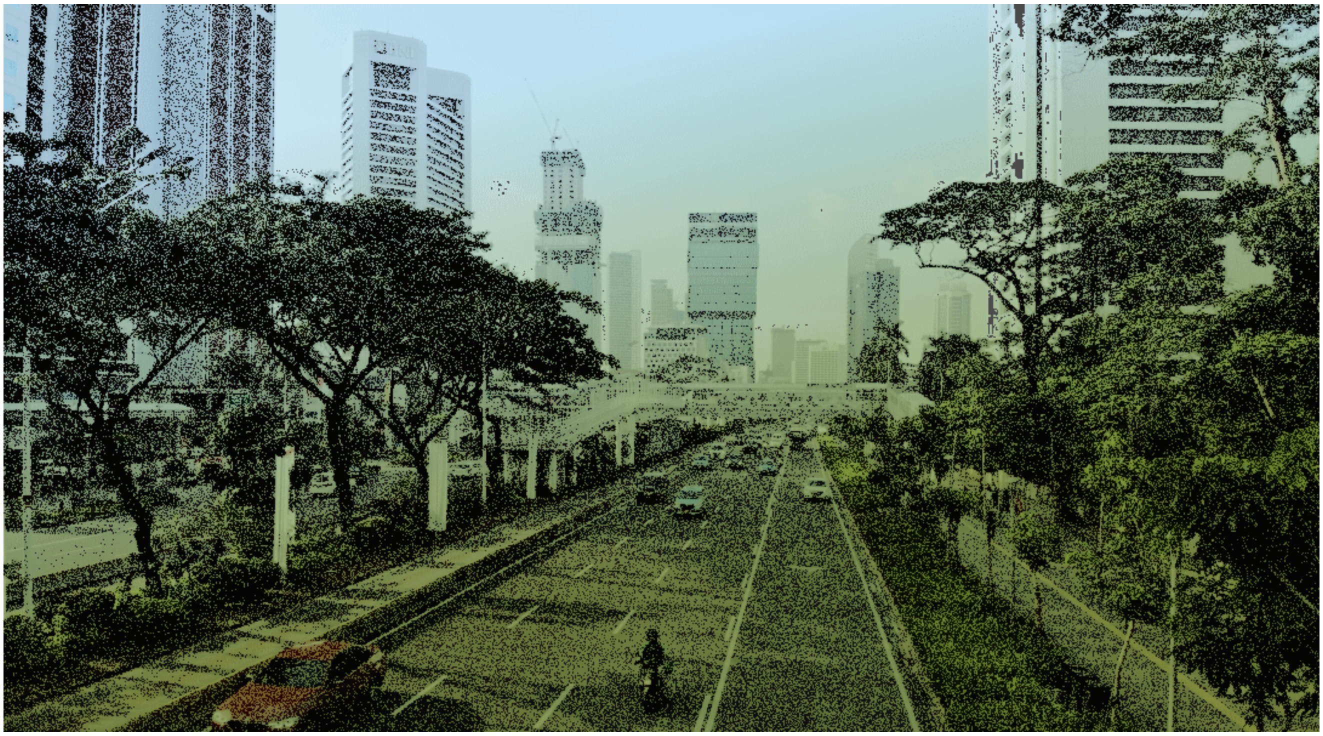

Image: Afif Kusuma, The Record

Chinese hackers have breached the internal networks of at least ten Indonesian government ministries and agencies, including computers from Indonesia's primary intelligence service, the Badan Intelijen Negara (BIN).

The intrusion, discovered by Insikt Group, the threat research division of Recorded Future, has been linked to Mustang Panda, a Chinese threat actor known for its cyber-espionage campaigns targeting the Southeast Asian region[1, 2].

Insikt researchers first discovered this campaign in April this year, when they detected PlugX malware command and control (C&C) servers, operated by the Mustang Panda group, communicating with hosts inside the networks of the Indonesian government.

These communications were later traced back to at least March 2021. The intrusion point and delivery method of the malware are still unclear.

Some systems are still infected, despite clean-up efforts

Insikt Group researchers notified Indonesian authorities about the intrusions in June this year and then again in July. Officials did not provide feedback for the reports.

BIN, which was the most sensitive target compromised in the campaign, did not return requests for comment sent by *The Record* in July and August.

A source familiar with the investigation told *The Record* last month that authorities had taken steps to identify and clean the infected systems.

Days after, Insikt researchers confirmed that hosts inside Indonesian government networks were still communicating with the Mustang Panda malware servers.

Part of China sprawling cyber-espionage campaigns

News of this intrusive cyber-espionage effort comes as the two countries have been re-establishing close diplomatic relations after almost reaching armed conflict a few years before, primarily due to marine territorial disputes.

Currently the second-largest investor in Indonesia, China has been cozying up to Indonesian provinces over the past two years to facilitate increased trade and further its implementation of the Belt and Road Initiative, a foreign policy initiative to invest in neighboring countries in order to establish lasting political ties and trade agreements.

But these investments haven’t always been welcome, with some countries seeing them as a Trojan horse for their economies.

Since 2013, when China made its Belt and Road Initiative public, cyber-espionage groups have often targeted countries where China planned to invest as part of this project.

Tags

- APT
- Badan Intelijen Negara
- BIN
- China
- Indonesia
- Mustang Panda
- nation-state
- PlugX

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.