Malaysia warns of Chinese hacking campaign targeting government projects

By Written by Catalin Cimpanu, ContributorContributor Feb. 6, 2020 at 5:25 p.m. PT

Archived: 2026-04-05 18:50:00 UTC

Image:Azlan Baharudin

Special feature

A Chinese state-sponsored hacking group has been targeting Malaysian government officials, computer experts with the Malaysian government said on Wednesday.

The purpose of the attacks has been to infect computers of government officials with malware and then steal confidential documents from government networks, Malaysia's Computer Emergency Response Team (MyCERT) said in a security advisory.

Attacks pattern

The attacks against government officials consist of highly-targeted spear-phishing emails.

MyCERT says the attackers have been pretending to be a journalist, an individual from a trade publication, and representatives for a military organization and non-governmental organization (NGO).

The emails contained links to documents stored on Google Drive. The documents, when opened, asked recipients to enable macros.

The malicious macros used two Office exploits (CVE-2014-6352 and CVE-2017-0199) to execute malicious code on the victim's system to download and install malware.

"The group's operations tend to target government-sponsored projects and take large amounts of information specific to such projects, including proposals, meetings, financial data, shipping information, plans and drawings, and raw data," MyCERT said.

MyCERT officials didn't say if government officials were compromised in these attacks.

Indirectly pointing the finger at China

However, while MyCERT didn't accuse the Chinese government directly, their advisory included links to research from the cyber-security community.

The write-ups [1, 2, 3, 4] describe the hacking tools and modus operandi of a cyber-espionage group known as APT40, known for its hacking activity alligned with the interests of the Chinese government.

In an exposé published last month, an online group of cyber-security analysts calling themselves Intrusion Truth have claimed that APT40 are contractors hired and operating under the supervision of the Hainan department of the Chinese Ministry of State Security.

According to FireEye, besides Malaysia, the group has also targeted Cambodia, Belgium, Germany, Hong Kong, Philippines, Norway, Saudi Arabia, Switzerland, the United States, and the United Kingdom.

The group has been primarily focused on "engineering, transportation, and the defense industry, especially where these sectors overlap with maritime technologies."

The APT40 group is also tracked by other security firms, but under other names, such as TEMP.Periscope, TEMP.Jumper, Leviathan, BRONZE MOHAWK, GADOLINIUM. The group has been active since 2014, according to multiple reports.

Security
