APT 30 government hacker group might not be from China

We shouldn't be so quick to point the finger

By **Lee Bell**

Wed Apr 15 2015, 10:16

THE APT 30 HACKER GROUP - which is said to have spied on Asian governments for over a decade - might not actually be from China.

The threat group was discovered and detailed by FireEye in its latest report earlier this week, claiming that it has been spying on Asia Pacific countries' governments from as far back as 2004.

FireEye's *APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation* report (PDF) said it believed the activity to be state sponsored, and said it is most likely the Chinese government.

But, while FireEye itself doesn't state that APT 30 is definitely Chinese, Malwarebytes highlights that we shouldn't be so quick to point the finger. The security firm's head of Malware Intelligence, Adam Kujawa, told *The INQUIRER* that as attribution is always difficult in the case of APT campaigns "because there is very rarely a smoking gun".

He said: "There are a number of factors in the report which seemingly point to Chinese involvement, but it is impossible to be definitive as these can always be 'false flags'.

"An interesting similarity that could be made is with the incident with a US EP-3 aircraft which crash landed in China in 2001. This ended with the disputed aircraft coming back in pieces after seemingly being reverse engineered."

FireEye claimed that APT 30 takes a special interest in political developments in Southeast Asia and India, and is particularly active at the time of Association of Southeast Asian Nations summits. It also focuses on regional issues and territorial disputes between China, India and Southeast Asian countries.

According to the security firm, the group has consistently targeted Southeast Asia and India over the past 10 years, prioritising their targets, working in shifts in a collaborative environment, and building malware from a development plan.

APT 30 is also said to target media organisations and journalists who report on topics concerning the region.

"We have analysed over 200 malware samples and its GUI-based remote controller software, and we are able to assess how the team behind APT 30 works," FireEye said.

"Their missions focus on acquiring sensitive data from a variety of targets, which possibly include classified government networks and other networks inaccessible from a standard internet connection."

APT 30 has not disclosed where its members reside, but FireEye said that its actions suggest Chinese involvement.

"Much of [APT 30's] social engineering efforts suggest the group is particularly interested in regional political, military and economic issues, disputed territories, and media organisations and journalists who report on topics pertaining to China and the government's legitimacy," said the FireEye report.

The white paper also said that, while attribution is always difficult, evidence suggests that APT30 may be sponsored by the Chinese authorities.

"Such a sustained, planned development effort, coupled with the group's regional targets and missions, leads us to believe that this activity is state sponsored, most likely by the Chinese government," read the report.

The group reportedly infects victims using phishing messages, and deploys a sophisticated set of attack tools and backdoors that have been developed over the past 10 years.

FireEye said that some malware being used by APT 30, primarily Backspace, shows characteristics of a modularised development framework.

"Our investigations into special tools - Shipshape, Spaceship and Flashflood - used by APT 30 suggest that, while they are not the only group to build functionality to infect and steal data from air-gapped networks, they appear to have designed this feature at the beginning of their efforts in 2005," said FireEye. µ

< Previous article | Next article >

Most read | Most commented | Most watched

John McAfee unlocks an iPhone and does not eat a shoe

Galaxy S7 specs, release date and price

Microsoft supports more handsets in Windows 10 Mobile Build 10586.122

The Pirate Bay reaches out to Kanye West

Windows 10 is now the second most popular desktop operating system