Lizard Squad threat no joke, security experts tell MAS after hacking

BY ZURAIRI AR

A screen capture showing the main page of MAS' website which was replaced by a photo of Airbus A380 jetliner bearing MAS' logo, with the words '404 — plane not found'

KUALA LUMPUR, Jan 27 — A group of online security firms has warned national carrier Malaysia Airlines Systems Bhd (MAS) against taking lightly the threat of hacker group Lizard Squad, which had threatened to leak confidential data from its servers.
According to Russia-based InfoWatch Group, the threat of targeted attacks on companies to leak data is growing "like an avalanche" over the past few years, with analysts claiming that the threat is one of the most common reasons for the leaks.

"As we can see now, the threat was more than real. Hackers have already released some confidential data that they claim they got as a result of the targeted attack on Malaysian Airlines," InfoWatch's spokesman Vadim Kuznetsov told *Malay Mail Online* in an email interview last night.

MAS' website was hacked and defaced yesterday, with hacker group Lizard Squad taking responsibility for it on its Twitter account @LizardMafia.

The group also tweeted "Going to dump some loot found on http://www.malaysiaairlines.com/ servers soon", likely referring to leaking private information of customers stored on MAS' servers.

It later posted an image of what is believed to be the national career's email system, which lists, among others, an urgent flight reservation for the International Trade and Industry Minister Datuk Seri Mustapa Mohamed.

The image also lists a number of travel itinerary receipts containing the full names of passengers, their email addresses and contact numbers.

“This could be the ‘loot’ that they are referring to. This is a serious threat as confidential data is often linked to financial data, while the schedule of travelling passengers is another can of worms altogether,” said Kuznetsov, who is also InfoWatch International sales director.

InfoWatch however could not comment on Lizard Squad’s motives for the attack, suggesting that most hackers do it for fame and financial gains.

“Hackers often make some part of stolen information public to prove the seriousness of their threats and then try to sell the other part of information back to victims or competitors,” Kuznetsov offered.

Lizard Squad had used the name “Cyber Caliphate” for the hack and had replaced the page’s title with the words “Isis will prevail”, likely in reference to the militant group now known as Islamic State.

InfoWatch however could not comment whether the group has any links with IS, or whether it was related to a previous attack on the US Central Command earlier this month by another group also calling itself Cyber Caliphate.

Source