Hackers who hit US media are back: security firm

WASHINGTON, US: The hackers who penetrated the computer network of The New York Times last year have resurfaced with an attack on "an organisation involved in shaping economic policy," experts have warned.

The security firm FireEye said the original perpetrators "appear to be mounting fresh assaults that leverage new and improved versions of malware."

Revelations about the attacks on The New York Times and Wall Street Journal heightened tensions between Washington and Beijing, prompting harsh comments from the White House and other US officials.

Chinese officials repeatedly denied responsibility for the attacks, and since then the United States has in turn been accused of penetrating foreign networks through the spy programs revealed by leaker Edward Snowden.

FireEye said it had detected "a retooling of what security researchers believe is a massive spying operation based in China."

"The new campaigns mark the first significant stirrings from the group since it went silent in January in the wake of a detailed expose of the group and its exploits," FireEye researchers Ned Moran and Nart Villeneuve said in a blog post.

FireEye said its researchers "spotted the malware when analysing a recent attempted attack on an organisation involved in shaping economic policy."

The name of the organisation was not disclosed.

The security firm said the malware "uses new network traffic patterns, possibly to evade traditional network security systems."

The New York Times said in January that hackers stole its corporate passwords and accessed the personal computers of 53 employees after the newspaper published a report on the family fortune of China's Premier Wen Jiabao.

The Wall Street Journal said later its computers were also hit by Chinese hackers. The Journal said in a news article that the attacks were "for the apparent purpose of monitoring the newspaper's China coverage" and suggest that Chinese spying on US media "has become a widespread phenomenon."

Source: AFP, via I-Net Bridge