THE WALL STREET JOURNAL.
WSJ.com

MEDIA & MARKETING | Updated January 31, 2013, 8:28 p.m. ET

Chinese Hackers Hit U.S. Media

Wall Street Journal, New York Times Are Breached in Campaign That Stretches Back Several Years

By SIOBHAN GORMAN, DEVLIN BARRETT and DANNY YADRON

WASHINGTON—Chinese hackers believed to have government links have been conducting wide-ranging electronic surveillance of media companies including The Wall Street Journal, apparently to spy on reporters covering China and other issues, people familiar with the incidents said.

Journal publisher Dow Jones & Co. said Thursday that the paper's computer systems had been infiltrated by Chinese hackers, apparently to monitor its China coverage. New York Times Co. disclosed Wednesday night that its flagship newspaper also had been the victim of cyberspying.

Chinese hackers for years have targeted major U.S. media companies with hacking that has penetrated inside newsgathering systems, several people familiar with the response to the cyberattacks said. Tapping reporters' computers could allow Beijing to identify sources on articles and information about pending stories. Chinese authorities in the past have penalized Chinese nationals who have passed information to foreign reporters.

Journal sources on occasion have become hard to reach after information identifying them was included in emails. However, Western reporters in China long have assumed that authorities are monitoring their communications and act accordingly in sensitive cases.

More

Hackers in China Targeted New York Times for 4 Months (New York Times)

Chinese Embassy spokesman Geng Shuang condemned allegations of Chinese cyberspying. "It is irresponsible to make such an allegation without solid proof and evidence," he said. "The Chinese government prohibits cyberattacks and has done what it can to combat such activities in accordance with Chinese laws." He said China has been a victim of cyberattacks but didn't say from where.

Foreign Ministry spokesman Hong Lei emphasized the point at a daily press briefing on Friday. "Cyber attacks are transnational and anonymous. It's very hard to trade the source of attack," he said. "To presume the source of a hacking attack based on speculation is irresponsible and unprofessional." He added that "Chinese authorities make serious efforts in fighting cyber

attacks."

The U.S. Federal Bureau of Investigation has been probing media hacking incidents for more than a year and considers the hacking a national-security matter. Investigators see it as part of a long-running pattern by a foreign entity to compromise the security of major U.S. companies, people familiar with the matter said.

Some evidence gathered in the probe suggested that the hacking was conducted largely by one group that focused on media companies, people familiar with the matter said. One person described the hacking as a swarm of relatively unsophisticated but persistent attempts to gain access.

"It's part of this overall story that the Chinese want to know what the West thinks of them," said Richard Bejtlich, chief security officer with the computer-security company Mandiant Corp., which was hired by the New York Times to investigate its breach. "What slant is the media going to take on them? Who are their sources?"

Mandiant, which is retained by companies to respond to cyberinfiltrations, said it has seen roughly 30 reporters and their managers targeted in incidents dating to 2008.

Bloomberg LP on Thursday said attempts had been made to infiltrate its systems but that its security wasn't breached. A spokeswoman for Thomson Reuters PLC said its Reuters news service was hacked twice in August. She said Reuters couldn't confirm the hacking source.

Computer-security firms that track Chinese cyberspying groups say that one of the roughly 20 groups they know about appears to specialize in the media industry.

"We know there are campaigns that are launched by specific groups targeting specific sectors," said Shawn Henry, president of CrowdStrike Inc., a computer-security firm. "When governments are actively collecting intelligence, they have developed subject-matter experts in particular industries," said Mr. Henry, a former FBI cybersecurity specialist.

The U.S. government has grown increasingly concerned about Chinese spying on the government and U.S. corporations, prompting U.S. intelligence agencies to issue a report a year ago calling Chinese hackers from the government and private sector the world's most "active and persistent" perpetrators of industrial spying.

Google Inc. and EMC Corp. computer-security unit RSA, among others, have said that their systems have been infiltrated. People familiar with those breaches said they were connected to the Chinese government.

The intelligence report discussed the extensive theft of data from global energy companies and proprietary data such as client lists and acquisition plans at other companies.

Cyberspecialists said the goals of hacking can include industrial espionage, insider trading and tracking potentially damaging information.

"The Communist Party really fears information and they can see their control unraveling as people read about corruption and officials with huge bank portfolios," said James Lewis, who advises U.S. officials on cybersecurity. "Information is an existential threat to these regimes."

The New York Times in an article Thursday detailed how Chinese hackers had infiltrated its systems over the past four months and gained access to passwords belonging to reporters and other employees. The paper said it believed it had expelled the hackers from its system.

Western companies, including media organizations, are reluctant to comment about possible Chinese hacking because they could lose customer confidence in their network security. Going public also risks antagonizing the Chinese government.

The Journal has faced hacking threats from China during the past few years, people familiar with the Journal investigation said.

In the most recent incident, the Journal was notified by the FBI of a potential breach in the middle of last year, when the FBI came across data that apparently had come from the computer network in the Journal's Beijing bureau, people familiar with the incident said.

The Journal hired consultants to investigate the matter and uncovered a major breach in which hacking groups—it wasn't clear whether they were working together—entered the company's networks, in part through computers in the Beijing office, people familiar with the situation said. The hackers then infiltrated the paper's global computer system, the people said.

Among the targets were a handful of journalists in the Beijing bureau, including Jeremy Page, who wrote articles about the murder of British businessman Neil Heywood in a scandal that helped bring down Chinese politician Bo Xilai, people familiar with the matter said. Beijing Bureau Chief Andrew Browne also was a target, they said.

The Journal began an investigation to track the cyberspies. The probe watched where the hackers went within the Journal's computer networks, what information they were interested in and how deeply they had penetrated.

A number of computers were totally controlled by outside hackers, who had broad access across the Journal's computer networks, people familiar with the matter said.

The investigation couldn't determine the full extent of the information that was spied on by the hackers, they said. The company's computer specialists erased several hard drives in Beijing last year.

"Evidence shows that infiltration efforts target the monitoring of the Journal's coverage of China and are not an attempt to gain commercial advantage or to misappropriate customer information," Paula Keve, a spokeswoman for Journal publisher Dow Jones, said in a written statement Thursday. Dow Jones is a unit of News Corp.

Data security is an "ongoing issue," Ms. Keve said. "We continue to work closely with the authorities and outside security specialists, taking extensive measures to protect our customers,

employees, journalists and sources."

The Journal in recent weeks has been taking steps to overhaul network security. The effort was completed Thursday.

—Jeffrey A. Trachtenberg
and Christopher S. Stewart contributed to this article.

Write to Siobhan Gorman at siobhan.gorman@wsj.com, Devlin Barrett at devlin.barrett@wsj.com and Danny Yadron at danny.yadron@wsj.com

A version of this article appeared February 1, 2013, on page B1 in the U.S. edition of The Wall Street Journal, with the headline: China Hackers Hit U.S. Media.