THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | FEBRUARY 5, 2011

Hackers Penetrate Nasdaq Computers

By DEVLIN BARRETT

Hackers have repeatedly penetrated the computer network of the company that runs the Nasdaq Stock Market during the past year, and federal investigators are trying to identify the perpetrators and their purpose, according to people familiar with the matter.

The exchange's trading platform—the part of the system that executes trades—wasn't compromised, these people said. However, it couldn't be determined which other parts of Nasdaq's computer network were accessed.

Investigators are considering a range of possible motives, including unlawful financial gain, theft of trade secrets and a national-security threat designed to damage the exchange.

The Nasdaq situation has set off alarms within the government because of the exchange's critical role, which officials put right up with power companies and air-traffic-control operations, all part of the nation's basic infrastructure. Other infrastructure components have been compromised in the past, including a case in which hackers planted potentially disruptive software programs in the U.S. electrical grid, according to current and former national-security officials.

"So far, [the perpetrators] appear to have just been looking around," said one person involved in the Nasdaq matter. Another person familiar with the case said the incidents were, for a computer network, the equivalent of someone sneaking into a house and walking around but—apparently, so far—not taking or tampering with anything.

A spokesman for Nasdaq declined to comment.

A probe into the matter was initiated by the Secret Service and now includes the Federal Bureau of Investigation.

The mystery surrounding the hackers and their motives is worrying investigators, who remain unsure whether they have been able to plug all potential security gaps—especially since invaders typically seek new ways to breach systems.

The case involving New York-based Nasdaq OMX Group Inc. is part of what cyber-crime authorities see as a broader problem of hackers nosing around corporate computer networks, with varying degrees of success.

U.S. companies are a continual target, and sometimes their public websites are vandalized. It is rarer for perpetrators to penetrate internal systems. Such breaches rarely come to light because companies fear that acknowledging them would alarm customers or encourage copycats.

Tom Kellermann, a former computer security official at the World Bank who now works at a firm called Core Security Technologies, said the most advanced hackers in the world are increasingly targeting financial institutions, particularly those involved in trading.

"Many sophisticated hackers don't immediately try to monetize the situation; they oftentimes do what's called local information gathering, almost like collecting intelligence, to ascertain what would be the best way in the long term to monetize their presence," he said.

People familiar with the Nasdaq matter said the Secret Service first began investigating last year. Investigators have informed White House officials of the case, according to the people familiar with the situation, who said that such a move is typical in hacking investigations, particularly in the early stages of the probes.

Authorities haven't yet been able to follow the trail to any specific individual or country. Those familiar with the case said that some evidence points toward Russia, but the person or people responsible could be almost anywhere, perhaps using computers in Russia merely as a conduit.

The case poses two concerns for authorities: preserving the stability and reliability of computerized trading, and ensuring that investors have full faith in that system.

Stock exchanges know they are frequently targets for hackers.

"We take any potential threat seriously and we are continually working to ensure that our systems operate at the highest levels of security and integrity," said Ray Pellecchia, a spokesman for NYSE Euronext, which operates the New York Stock Exchange.

He declined to discuss any specific instances of computer-hacking attempts against that exchange.

In 1999, hackers vandalized Nasdaq's publicly accessible website. In that incident, a group of hackers quickly claimed responsibility for defacing the site, as well as major media websites. Nasdaq officials at that time said the company's internal network wasn't affected.

Computer hacking is a problem for many countries. In recent years, U.S. authorities have dealt with cyberattacks linked to computers in Russia, China and Eastern Europe.

Hackers can use geography as a foil. Prosecutors said Albert Gonzalez, perhaps the most renowned hacker, perpetrated his biggest theft with help from computers in Eastern Europe even though he lived in Miami.

According to a 2009 federal indictment, he used computers located in the U.S., Latvia and Estonia, in a conspiracy that netted more than 100 million stolen credit-card numbers.

The case is considered the largest hacking crime in U.S. history. Mr. Gonzalez eventually pleaded guilty and was sentenced to 20 years in prison.

Write to Devlin Barrett at devlin.barrett@wsj.com