Hacking fears raised by Nasdaq OMX attack

Print

By Philip Stafford, Jeremy Grant and Telis Demos
Published: February 7 2011 21:33 | Last updated: February 7 2011 21:33

Nasdaq OMX's confirmation that it has been targeted by hackers has thrown the spotlight firmly on IT security at the world's exchanges, a crucial part of many countries' **capital markets**.

But does that mean it is possible for hackers, even cyberterrorists, to bring down an exchange, causing financial mayhem?

Nasdaq said over the weekend that it had discovered "suspicious files" on servers, but that these were unrelated to its trading systems. It said that its "web-facing" application, called Directors Desk, was "potentially affected".

Breaking into an **exchange's trading system** would be extremely hard, experts say, because exchanges have developed multiple layers of security to stop that happening. They involve complex software protocols and the use of algorithms that constantly, and randomly, change security codes.

Many exchanges run on a separate private network, often with its own computing language. To trade on the London Stock Exchange, for example, one must be a member or be given access via a broker, known as "sponsored access".

Any new trading firm would then have to mesh their networks to the trading venue. Each layer requires extensive background checks and testing. "There are controls for anything that is fundamental to trading between buyer and seller," says Bob Fuller, a director of Fixnetix, a trading technology company.

A more plausible threat is one where an exchange is bombarded with trades from a pre-programmed computer algorithm. The "flash crash" in US markets last year was triggered by an algorithm in the futures markets which malfunctioned, sending the Dow Jones average down 1,000 points – and back up again – in 20 minutes.

Safety catches known as circuit-beakers are now in place to help prevent a disaster. Last week Mary Schapiro, chairman of the Securities and Exchange Commission, said the agency was now looking beyond that and considering tougher brakes known as "limit-up/limit-down style trading parameters".

Yet the attempted hacking on Nasdaq has sparked broader concerns about information security, particularly for data that can be stolen and used for insider trading. Last week, trading on Europe's carbon markets resumed after the alleged theft of €30m ($40.7m) of carbon trading permits from national registries.

In the Nasdaq case, it was an online registry that was targeted, called Directors Desk. The service is a web-based "cloud" application that stores data of thousands of Fortune 500 companies that are only supposed to be accessed by authorised users such as the directors of the companies themselves. In other words, it is a rich mine of market-moving, inside information.

No details of how the alleged hacking into Europe's carbon emissions permits have emerged but experts suspect that passwords used by corporate traders such as cement groups and manufacturers have been passed to sophisticated organised criminals.

"This is definitely something that is targeted based on a specific reward," says William Beer, director at One Security, the IT security practice at PwC, a consultancy group.

Directors Desk is an example of a phenomenon that is growing at exchanges:

Markets under attack

- **September 1999** Hackers break into computers used to operate the w ebsites for American Stock Exchange and Nasdaq, leaving messages on the system.
- **2004** Van Dinh, a 19-year-old living w ith his parents in Pennsylvania, is sentenced after online trading hacking and identity fraud.
- **October 2007** A Ukrainian engineering consultant named Oleksandr Dorozhko hacked into a computer that contained advance information about a negative earnings announcement from IMS Health.
- **October 2009** Van Dinh pleads guilty to cracking a New York-based currency exchange service and gifting himself more than $100,000.
- **January 2011** European Commission halts emissions trading system for tw o w eeks follow ing allegations of theft of permits from European carbon trading market.
- **February 2011** Nasdaq OMX targeted by hackers w ho breached its system but did

offering extra services, often web-based, as a way to attract companies to list. Nasdaq offers these under a package it calls “corporate solutions”, including a service aimed at company investor relations staff that integrates corporate shareholder communications, capital market information and “board-level reporting” – all on one computer screen.

not compromise its trading operations.

Yet the vulnerability of Directors Desk has highlighted tension between the competitive pressures exchanges are under to offer such services online, and the risks that they can be hacked for insider trading. “It’s a question of what people are willing to put in a semi-secure area to promote business,” says a senior executive at a rival European exchange. “It’s also a question of what is at risk when someone gets into that environment.”

NYSE Euronext has a similar service called eGovDirect.com but it was taken down last week for maintenance and has yet to return. NYSE said the issue was technical and not related to the Nasdaq issue. “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,” it said.

Experts say web-based services act as a back door for hackers and, as in the carbon market, one of the most lucrative ways is by hacking existing, credible and normally trustworthy names. As new products like computer tablets emerge, the proliferation of internet-based “apps” makes hacking more likely.

“Two major developments that are creating risks for clients are the cloud and mobile,” says Mr Beer. “[Exchanges] are trying to have that flexibility. But it’s introducing new risks.”

“It was inevitable,” says Justin Magruder, chief executive of Noetic Partners, which builds trading data systems. “Virtualisation is a relatively new application and is very complex. My assumption is that most clouds are vulnerable because of the sheer number of access points, and many have already been hacked. We just don’t hear about it.”

Directors Desk: ‘No files breached’

Directors Desk, the website that was the source of the attempted hacking at Nasdaq, is part of a suite of corporate services that Nasdaq offers to attract issuers to its marketplace, **writes Telis Demos**.

Nasdaq acquired the company in 2007. It provides web-based collaboration tools to some 5,000 companies, enabling executives and board members to share documents, communicate and vote on proposals.

On its website, it says it complies with international security standards, “providing multiple levels of protection to guard our clients’ confidential data against undesired access”.

On Monday morning, Directors Desk sent out a message to clients acknowledging the attempted breach, but said that no files were compromised.

“Clients right now are probably doing a damage assessment, asking what’s up there that could hurt them,” said Wayne Matus, a partner at Pillsbury.