By Jud Welle, Nicholas Peck & Scott Nawrocki

Hack & Sell Short: A New Cyber Threat

A recent piece in the *Financial Times* drew attention to the potential for short sellers to drive down a company's share value by conspiring with hackers to attack a target company's IT systems. The author of the article made the urgent but underappreciated observation that the number of malign actors capable of sophisticated hacking has proliferated in recent years, in large part because rogue states have been willing to sell or provide such capabilities to financial criminals looking to reap a windfall.

As an investigative firm with extensive experience dealing with both cyber and short selling investigations, it's our view that the threat of cyber-enabled short selling is very real. Unscrupulous securities traders have proven all too eager to conspire with hackers to secure an illegal advantage in the market. According to a federal indictment, between 2010 and 2015, a group of hackers pilfered documents detailing transactions involving publicly traded companies ahead of their public announcement and shared them with co-conspirators. The latter, among them SEC registered broker-dealers, leveraged the not-yet-public information to make trades in the underlying stocks, while cutting the hackers in on a share of the profits. The same scheme could easily be adapted to short selling, with the added advantage (from the criminals' point of view) that advance knowledge of a hacking attack is easier to conceal than receipt of confidential documents.

Recent market trends have created favorable conditions for such a cyber/short-attack scheme. Major US stock indices have reached record highs, setting up many stocks for a precipitous drop in price should the company suffer a cyber attack. In addition, initial public offerings have been coming at a record clip as companies list their shares directly on exchanges or go public via special purpose acquisition companies (SPACs), increasing the number of targets for cyber-enabled short selling. Finally, pandemic-induced changes to business operations, including expanded reliance on remote work platforms, have increased companies' vulnerability to being hacked.

Who is Vulnerable? Not Necessarily Who You'd Think.

Firms whose business models don't depend on protecting trade secrets or sensitive data could be forgiven for thinking they aren't in the crosshairs of hackers and their short selling accomplices. The notion that *if we don't have anything worth stealing, we won't be hacked* has gone out the window with the rise of ransomware.

Ransomware attackers profit not by selling stolen data, but by crippling corporate networks and holding a company's operations hostage until it pays the attackers a hefty sum. Such attacks have proven quite lucrative for hackers, but that may change as US authorities threaten sanctions against organizations, ranging from banks and insurance companies to incident response consultancies, that facilitate victims' ransomware payments to these criminals. Shorting offers hackers a way to profit from their handiwork without having to secure a ransom payment or find a buyer for stolen data. If their attacks drive down the share price of their victims, they're in the money.

Ironically, the targets of such a ransomware-enabled short attack may be those firms least concerned about being hacked. Why go after a company that has invested in cyber defenses to defend its data when you could attack one that has left its IT infrastructure unguarded?

For this reason, the companies most at risk of cyber-enabled short sellers are young, growth-oriented firms whose cyber defenses are lagging those of their more mature counterparts. Attaining effective IT security takes time and money and there are no shortcuts. Security cannot be bought off the shelf and only comes about through governance, investments in people and technology, and senior management's commitment to creating a culture of security. In the pursuit of rapid growth, some companies may have had neither the time nor inclination to prioritize security. Indeed, they may have shunned security improvements as a drag on their agility and creativity.

What Can Companies Do?

While short sellers often publicize the reasons for their position in order to move the market, they are obviously unlikely to advertise when they have illegally coordinated or carried out a cyber attack. To that end, cyber short selling investigations require three key steps:

- Identify the parties behind the relevant hack.
- Identify the parties making short selling attacks.
- Prove that both parties have worked in concert to profit from the decline in share price at the targeted company.

Of course, rather than investigate after the fact, companies should look to how they can minimize their exposure to these types of attacks. Companies at risk can take the following steps to prepare for and plan their response to cyber-enabled short selling:

- Conduct a cyber risk assessment that encompasses critical third-party vendors and cloud platforms and take remedial action to address vulnerabilities.
- Research online sources, including the Deep/Dark Web, for chatter that may signal the company is being targeted for attack by either hackers or short sellers.
- Run a tabletop exercise that prepares security teams and management for a prospective short seller-driven cyber attack.
- If malicious activity is uncovered, be ready to engage a partner with the expertise and capabilities to investigate the tactics, techniques, and procedures of both hackers and short sellers.

Collusion between short sellers and hackers poses steep risks for publicly traded companies and their shareholders. Planning and prevention are key: mitigating these risks hinges on not selling short the creativity and sophistication of today's cyber criminals.

About our firm

Nardello & Co. is a global investigations firm whose experienced professionals handle a broad range of issues including due diligence, anti-corruption & fraud investigations, civil and white collar criminal litigation and arbitration support, asset tracing, activist defense, political risk and strategic intelligence, digital investigations and cyber defense, monitorships and independent investigations, and compliance. Nardello & Co. has been recognized as a top-tier firm by Chambers and Partners worldwide and is the only investigative firm in the US to earn a Band 1 ranking, their highest level of recognition.

Our clients include the world's leading law firms and financial institutions, Fortune 500 and FTSE 100 companies, high-net-worth individuals and family offices, governments, NGOs, sports organizations, and academic institutions.

With offices in New York, London, Washington DC, Hong Kong, Tokyo, Milan, and Dubai, Nardello & Co. maintains a professional staff that includes former US federal prosecutors, US and international lawyers, former law enforcement personnel and intelligence operatives, licensed investigators, research analysts, former journalists, financial crime specialists, forensic accountants, and computer forensic experts.

Contact

Jud Welle
Managing Director, Head of Digital Investigations & Cyber Defense, and Chief Counsel, Cybersecurity & Privacy
+1 212 537 5300
jwelle@nardelloandco.com

Nicholas Peck
Senior Managing Director
+1 212 537 5300
npeck@nardelloandco.com

Scott Nawrocki
Managing Director, Digital Investigations & Cyber Defense
+1 212 537 5300
snawrocki@nardelloandco.com

Nardello WE FIND OUT & Co.