Shorting, reporting and profiting in the era of cyber security

Recent short seller collaborations with security researchers demonstrate a new trend in the evolving short seller strategy of publishing harmful information about a company and profiting from the drop in stock price. This new trend involves a public disclosure of information about a material cyber security vulnerability in a target company's products or IT systems. This disclosure of information often results in an immediate drop in the target company's stock price. Short sellers stand to gain millions from these efforts in a matter of minutes with potentially lasting financial impact on targeted companies. Todd S. McClelland and Frances P. Forte of Jones Day explore the implications of this trend, and discuss mitigation approaches for those businesses that could be affected by such strategies.

The trend described in the introduction, however, is only a slight evolution of similar short seller strategies we have been observing for some time. More recently, short sellers have been engaging in 'doxing' by exploiting the wealth of information that is readily available about companies and individuals over the internet, including social media. Normally, doxing involves researching and compiling personally identifiable or sensitive information about a specific person or company and then using it with malicious intent. For example, during the Ferguson protests, the hacker-activist group Anonymous began releasing the identities and personal information of Ku Klux Klan members[1].

Methods for doxing companies are becoming more sophisticated. Professional researchers have started using open source and other internet-based data to effectively manipulate a target company's overall stock price. If researchers and short sellers collaborate to short a target company's stock by publishing a report with potentially damaging information about the company, they stand to realise significant profits if the company's stock drops.

The advancement of this doxing trend into the cyber security space is capturing the attention of internet-based technology providers, especially providers of so called 'Internet of Things' ('IoT') products. In this emerging model, a security researcher finds a vulnerability affecting an IoT product. Rather than share the discovery with the product's provider, a financial arrangement is reached between the security researcher and a short seller. The short seller or security researcher publishes the researcher's findings, and the short seller and security researcher share in the profits as the company's stock price falls. Perhaps the most public example of this model reported to date involves St. Jude Medical, Inc. ('St. Jude Medical') and an investment report released by Muddy Waters Capital LLC ('Muddy Waters'), discussed at greater length below.

The purpose of this article is to explore this emerging short seller model and provide practical considerations for companies potentially in the cross-hairs of these short seller and security researcher collaborations. This article begins with a discussion of the Quindell example to provide further background on the origins of this trend. We then discuss the events involving St. Jude Medical, and the impact an investment report on cyber security vulnerabilities had on the company. We conclude with a discussion of efforts providers of IoT products and others can proactively pursue to mitigate these and related risks[2].

Quindell PLC

Quindell, a London-based publicly traded company, saw its value plummet from about £2.4 billion to £1.5 billion in a single day after a research company, Gotham City Research LLC ('Gotham'), tweeted and released a report (the 'Gotham Report') regarding Quindell's financial status and other financial concerns[3]. The Gotham Report began by calling Quindell "[a] country club built on quicksand[4]." It dove into the financials of the company, using both public and non-public information collected from various sources, alleging, among other things, that Quindell's CEO spent £12 million to build a country club and further that Quindell's shares were uninvestable until the identified concerns in the Gotham Report were fully addressed[5]. The information cited in the Gotham Report was alleged to have been sourced from a vast array of sources such as the company's corporate filings and other public documents, and also social media sources such as LinkedIn and Twitter.

Immediately following release of the Gotham Report, Quindell's share price dropped almost 50%[6]. Given this significant financial impact, nothing suggests that short sellers will soon abandon the strategy employed by Gotham. With the increasingly large amount of open source, personal and embarrassing information available on the internet, we should expect that doxing-like strategies will be around for the foreseeable future.

St. Jude Medical, Inc.

On 25 August 2016, the investment research firm Muddy Waters announced it would be heavily shorting St. Jude Medical, a global medical device manufacturer[7]. Muddy Water's investment report (the 'MW Report') stated that St. Jude Medical's implantable cardioverter defibrillators ('ICDs'), cardiac resynchronisation therapy implantable cardioverter defibrillators ('CRT-Ds'), and pacemakers should be recalled and remediated because they have significant security vulnerabilities that could be easily exploited by hackers[8].

Todd S. McClelland Partner
tmcclelland@jonesday.com

Frances P. Forte Associate
fforte@jonesday.com

Jones Day, Atlanta

The MW Report cited two demonstrations of cyber attacks against the ICDs:

- a 'crash' attack that causes ICDs to malfunction - including pacing at a potentially dangerous rate; and
- a battery drain attack that could be particularly harmful to device-dependent users[9].

Further, the MW Report stated that the devices lacked basic encryption and authentication protections, and as a result, a hacker could impersonate any one of the devices and likely communicate with St. Jude Medical's internal network[10]. The MW Report alleged that hackers' 'keys to the castle' (i.e., the monitoring units) were readily available on eBay for no more than $35[11]. Muddy Waters strongly projected that St. Jude Medical may lose half of its revenue over the next two years (the estimated two-year remediation time) since the ICDs, CRT-Ds, and pacemakers accounted for almost 50 percent of St. Jude Medical's revenue in 2015[12]. Muddy Waters asserted that these vulnerabilities are more worrisome than medical device hacks publically discussed in the past, claiming that the attacks can be directed at ICDs within a 50 foot radius and theoretically executed on a very large scale, putting hundreds of thousands of lives at risk[13].

Within 90 minutes of Muddy Water's announcement, St. Jude Medical's stock fell more than 8%[14]. It was later reported that prior to taking a short position on St. Jude Medical's stock, Muddy Waters had formed a financial arrangement with MedSec Holdings, Ltd. ('MedSec'), a self-proclaimed 'white hat' hacking group. MedSec alleged that it had the data to prove that St. Jude Medical's devices have vulnerabilities that "could result in permanent impairment, a life-threatening injury, or death[15]." Based on MedSec's research, Muddy Waters took a short position on St. Jude Medical's stock, predicting that the share price would fall when they published the research. MedSec's fees were reportedly based on Muddy Water's rate of return on the investment[16]. Essentially, this financial arrangement meant that the worse MedSec characterised St. Jude Medical's cyber security vulnerabilities, the more money Muddy Waters stood to make (since it shorted the stock), which in turn would lead to greater profits for MedSec.

After information about the relationship between MedSec and Muddy Waters was released, many investors looked upon the MW Report with scepticism, noting its inherent bias. St. Jude Medical subsequently sued Muddy Waters and MedSec alleging defamation, deceptive trade practices, and civil conspiracy arising from "Defendants' intentional, wilful and malicious scheme to manipulate the securities markets for their own financial windfall through an unethical and unlawful scheme premised upon falsehoods and misleading statements initially contained in an 25 August 2016 Muddy Waters report [...][17]."

Mitigation approaches

The security of IoT and other connected products is a growing concern for everyone. The emerging short sale trend experienced by St. Jude Medical is one of just a number of challenges IoT and other connected product providers face every day.

In addition to the various legal challenges product providers might pursue in the wake of a disclosure by a short seller or security researcher, product providers can employ a number of preventative and proactive measures both during the product development process and after the public distribution of their products that have the potential to greatly reduce the overall impact of this short seller strategy. A few examples of these measures include the following:

- Security is often an overlooked component of many product development efforts. Incorporating security considerations (e.g., threat modelling) during the product architecture and early design phases can make a product considerably more secure and reduce the likelihood that security researchers find reportable vulnerabilities. Of course, security considerations should be considered during the full course of the product development lifecycle, especially during product testing and evaluation. This suggestion is bolstered by the National Institute of Standards and Technology's ('NIST') recently released guidance that urges IoT product providers to build strong security protections into products at the outset[18].
- Many vulnerabilities first come to light once a product is released to the public. This is also the time when security researchers have their first access to a product and can perform their own testing of a product.

continued

Accordingly, product providers should consider an ongoing program to take in, identify, address, and remediate security vulnerabilities.

- Many products, once sold or deployed, are not capable of having their firmware or software updated to address identified vulnerabilities. As a result, the only course of action for a material vulnerability may be a full product recall and replacement. Enabling remote or even local patching or updating of a product can be considerably less expensive than doing a full product recall and replacement. Accordingly, while a product may have a vulnerability, if a simple patch or update can be readily implemented, the overall impact on the company could be relatively minor.
- In some circumstances, security researchers have legitimate concerns both that companies are not interested in learning about product vulnerabilities, and that the vulnerability could be life-threatening or otherwise of great public interest. By developing a process to receive and act on vulnerabilities, companies can better challenge this researcher argument and potentially avoid a larger problem later on.
- Many companies are proactively engaging security researchers to help them identify vulnerabilities or bugs in their products. These 'bug bounty' programs incentivise security researchers (often financially and with attribution) to share their research directly with the company. Many such programs are structured to provide the company with a reasonable period of time to release a patch or update, thereby correcting the problem, before the vulnerability is made public. More and more companies are announcing bug bounty programs, and the cash rewards are increasing. In August, for example, Apple announced to Black Hat attendees that it will offer cash bounties of up to $200,000 to researchers who discover vulnerabilities in its products[19]. Such significant bounties help give security researchers another lucrative channel to profit from their efforts. They also provide product developers ready access to global research talent without the need to hire additional employees.
- Industry standards and guidelines offer additional assistance for providers of IoT and other connected products to manage cyber security related risk. As noted above, the NIST Special Publication 800-160 offers guidance for makers of IoT products to help build robust security protections into IoT products and contains systems security considerations for system and software engineering, focusing on a system life cycle process[20]. NIST urges IoT providers not to "focus on what is likely to happen - but instead, focus on what can happen and be prepared[21]." This means proactively planning and designing with cyber security standards and considerations in mind from the outset so that product providers can be in an informed and better structured position to quickly recover from vulnerability disclosures and other incidents when they happen.
- Companies are increasingly adopting incident response plans to facilitate and guide their response to attacks on corporate IT systems. Yet, many product providers do not have a similar response plan in place to address attacks on their products, disclosures of material vulnerabilities, or other incidents affecting their products. Companies should consider having such a plan in place, and if possible, test the plan to optimise it for success should such an incident occur.

Conclusion

The threat of security researchers and short sellers colluding for financial gain is not likely to go away any time soon, and it is likely to expand. We expect that reports will continue to surface of similar short seller strategies involving the disclosure of alleged cyber security vulnerabilities in other systems and products, including for example corporate IT systems, critical infrastructure, and connected manufacturing systems (e.g., the 'industrial internet'). Companies at risk should prepare.

IoT and other connected product providers in particular must be especially mindful of these risks. Such providers, therefore, should be proactive in taking preventative measures, which may include those measures mentioned above, against product vulnerabilities, or otherwise run the risk of being shorted, their vulnerabilities reported, and their share price affected.

The views and opinions set forth herein are the personal views or opinions of the authors; they do not necessarily reflect views or opinions of the law firm with which they are associated.

With contributions from Aditya Shrivastava.

1. http://fox2now.com/2014/11/17/hacker-activist-group-anonymous-seizes-kkk-twitter-accounts-reveals-identities/
2. This article does not attempt to address the various legal claims companies might bring against short sellers and security researchers. Rather, we only attempt to address some risk mitigating approaches at-risk companies might implement to lessen the likelihood or impact of a vulnerability disclosure.
3. http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/insurance/10790021/the-day-gotham-citys-tweet-cost-quindell-1bn.html
4. https://www.scribd.com/doc/219517633/Quindell-PLC-A-Country-Club-Built-On-Quicksand#fullscreen&from_embed
5. Ibid.
6. http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/insurance/10790696/hedge-fund-manager-davide-serra-alleges-price-manipulation-in-shorting-attack-on-quindell.html
7. http://www.muddywatersresearch.com/wp-content/uploads/2016/08/MW_STJ_08252016_2.pdf
8. Ibid.
9. Ibid.
10. Ibid.
11. Ibid.
12. Ibid.
13. Ibid.
14. http://www.startribune.com/st-jude-stock-tumbles-as-report-questions-company-s-cybersecurity/391310831/
15. http://www.muddywatersresearch.com/wp-content/uploads/2016/08/MW_STJ_08252016_2.pdf
16. https://www.bloomberg.com/news/articles/2016-09-06/the-new-short-find-industries-exposed-to-exotic-hacking-attacks
17. St. Jude Medical, Inc. v. Muddy Waters Consulting LLC, No. 16-cv-03002 (D. Minn. filed 7 Sept 2016).
18. https://doi.org/10.6028/NIST.SP.800-160
19. http://www.forbes.com/sites/thomasbrewster/2016/09/28/apple-iphone-hacker-meet-cupertino/#1d085597e29f
20. https://doi.org/10.6028/NIST.SP.800-160
21. Ibid.