FOCUS

Vol. 26, Vol. 7 International Federation of Pharmaceutical Wholesalers April 11, 2019

Meeting the Threat: Cybersecurity for Pharmaceutical and Biotech Firms

(Source: An article by Megan Berkowitz for Automation.com)

In 2017, pharmaceutical manufacturer Merck was one of many companies targeted by a ransomeware attack known as "WannaCry". The attack, as reported by Reuters, caused massive disruptions to Merck's medicines and vaccines, costing the company millions of dollars. Additionally, it caused work disruptions for Merck's employees who rely heavily on computers to accomplish their work.

The WannaCry ransomware attack that successfully targeted Merck is not the only one to plague the pharmaceutical industry. The digitalization and storage of valuable data by pharmaceutical and biotech companies have allowed them to fall victim to hackers in ways not otherwise imagined years ago. These manufacturing facilities rely heavily on "the internet of things" and connected technology in order to automate their very precise and sensitive manufacturing processes, making them more susceptible to attack. These internet-connected endpoints must be protected in order to preserve the processes they support. Additionally, the proprietary information behind drugs and other biopharma advances are valuable and making them a high priority target. Every time this information is infiltrated by hackers, it undermines the trust and confidence of consumers and patients.

Across the industry, steps are being taken to step up companies' cybersecurity game. More and more resources are being deployed that incorporate cutting-edge technologies such as machine learning, artificial intelligence, and orchestration.

One very important question to consider is to what strategic ends are these cutting-edge technologies being put? Are they just a means of fortifying traditional methods of cybersecurity in order to create faster and more efficient versions of the same product, or are they being used in ways that are new and innovative?

Traditional cybersecurity focuses on reporting incidences after the intrusion has occurred, otherwise known as "incident responses". In these instances, the adversary, or hacker, gains access to the system and compromises it. These vulnerabilities can be found in web framework, internet browsers, or internet infrastructures/hardware such as routers and modems. Regardless of where the intrusion occurs, once the intrusion is discovered, the forensics about the attack, including basic information known as "Indicators of Compromise" (IOCs) such as IP addresses, domain names or malware hashes, are shared across the cybersecurity community. The IOCs are then used to thwart future attacks.

The issue is that this approach causes two problems. First, someone must be the victim of the attack so that IOCs can be established and shared with others. Second, most intruders subscribe to the very same feeds that companies employ, making it easy for them to realize when they have been discovered within the cybersecurity community. Once the intruder has been exposed, they need only to come up with a new IP address or recompile their malware so that it has a new hash value. This allows new attacks

(continued on page 2)

In Brief...

- **Walgreens Boots Alliance** announced solid sales of US$34.5 billion (a gain of 4.6% year-over-year) as well as strong retail pharmacy performance in the U.S., but industry-wide headwinds plagued the company in its fiscal second quarter. Net earnings decreased to US$1.2 billion, down 14.3% from the prior-year period. Executive vice chairman and CEO, *Stefano Pessina*, attributed the difficulties to reimbursement pressure and ldeflation, along with ongoing U.S. and U.K. consumer market challenges, calling it "the most difficult quarter we have had since the formation of Walgreens Boots Alliance." Pessina also said that the company would be pursuing various efforts to counteract headwinds, including senior appointments to help speed up the business' digitization and transformation, as well as cost-cutting initiatives.
- **McKesson Corporation** announced that *Brian Tyler*, a 22-year veteran of the company, would assume the role of *John Hammergren*, who has led the company as CEO since 1999 and will remain as board chairman for **Change Healthcare** while also supporting Change Healthcare as an advisor. McKesson also announced that *Edward Mueller* would be taking over the board of directors. Mueller previously served as lead independent director since 2013 and has served on McKesson's board since 2008. Seperately, McKesson announced that effective April 1st, its Las Colinas campus in Irving, Texas would serve as McKesson's headquarters.

(continued on page 2)

McKesson Announces Move to Google Cloud

(Source: PRNewswire)

McKesson Corporation announced a technology collaboration with Google Cloud which will advance the development of next-generation applications and products, machine learning and artificial intelligence (AI) technologies, and enhanced analytics in support of the company's strategic growth initiative aimed to transform healthcare delivery while also driving profit.

As part of the agreement, Google Cloud will become McKesson's preferred cloud provider. McKesson plans to implement the Google Cloud Platform (GCP) across its entire enterprise as the foundation for its new infrastructure, platforms, applications and analytics. This will result in not only greater efficiency for the company, but a significant cost savings as well.

"We're excited to work with Google Cloud to design a cloud infrastructure that frees us up to problem solve for the future of healthcare," said Andy Zitney, senior vice-president, and chief technology officer for McKesson Technology. "We are accelerating our migration and development process, which we will be able to deploy new products and features for our customers faster, decreasing our time to value. This collaboration will help us

(continued on page 2)

Copyright © 2019 - IFPW All Rights Reserved.

Cybersecurity (cont.)...

to sail through easily since defenses are dependent on IOCs and renders this "after-the-fact" approach as inherently flawed.

Since incident response only helps prevent attacks that exactly replicate past attacks, the cybersecurity industry needs to embrace a paradigm shift that is based on proactive implementation so that attacks are thwarted before they ever happen. This will require a sophisticated approach designed to successfully recognize adversary methodology before attacks occur, and at a meaningful scale. This kind of approach, when employed in tandem with incidence response tactics could provide true and real-time preventative security to critical networks within all industries. By shifting attention towards prevention, proactive cybersecurity analysts can instead use the information gleaned regarding adversaries' methodologies – commonly referred to as tactics, techniques and procedures (TTP). Analysts can identify the general form and components of adversarial campaigns through these TTPs. Additionally, they can determine abstract indicators such as how the adversary is attempting to hide its actions. Once a proactive cybersecurity tool is employed, it could recognize TTPs and indicators that describe threatening behavior in general terms, which in turn would allow it to act on any traffic that meets the identified pattern before it reaches the guts of the network. Also, this prevention plus response method of cybersecurity enables teams to truly take advantage of new and cutting-edge technologies in ways that change the game, putting companies on offense in the cybersecurity world.

With these two methods being used in tandem, cybersecurity teams could make meaningful headway in reducing the number of attacks and more quickly and effectively respond to attacks.

McKesson (cont.)...

more effectively capture, process and convert data into actionable business insights – as well as focus on automation freeing our engineers' and developers' time."

Specifically, the move to GCP will provide a more flexible architecture for McKesson to:

- Build a secure, scalable, highly-resilient environment with the agility and flexibility to meet business demand;
- Develop new modernized applications and solutions for product manufacturing, specialty pharmaceutical distribution, and retail operations for pharmacies;
- Capture and deliver real-time intelligence and insights with first-class cloud analytics tools;
- Expand capacity to integrate machine learning and AI into applications;
- Accelerate delivery of new services and ability to scale more rapidly; and
- Reduce infrastructure management and administration-freeing technology teams to focus on product and feature development.

With Google Cloud's capabilities, McKesson expects to accelerate implementation of cutting-edge technologies to market, along with improving long-term performance. Also, McKesson's cloud-first approach will transform ways in which the company manages its information services by transitioning it from a predominantly "in-house" operating model to a hybrid, cloud-based services model that will increase productivity.

In Brief (cont.)...

- **CVS Pharmacy** announced that it is kicking off its same-day, on-demand prescription delivery service, adding to its existing service of 1 to 2-day prescription service that is already available nationwide. The service, delivered by **Shipt**, is available at 6,000 CVS Pharmacy locations across the United States. Customers may opt for its On-Demand prescription delivery service through its CVS mobile app, SMS text or by calling their local CVS Pharmacy. The delivery service charge is US$7.99. Also included are thousands of the most popular health and house items, including over-the-counter medications, vitamins, baby and feminine care products.
- The generic utilization rate in Japan for October-December 2018 came in at a preliminary 74.7%, based on a volume basis, up 1.5 points over the previous quarter, according the **Japan Generic Medicines Association** (JGA). The generic rate generally represents the volume of generics shipped versus the total shipment volume of generics plus original drugs with generic substitutes. The quarterly share is based on data provided by **IQVIA**, as well as shipment data from JGA members. Separately, the Japanese ethical drug market was down 1.4% versus the previous year, according to a monthly snapshot report released by market research firm **Encise**, a subsidiary of **Crecon Research and Consulting**. Chugai Pharmaceutical's *Avastin* was the best-selling drug, followed by MSD's *Keytruda*. Pfizer's pain medication *Lyrica* closely trailed *Keytruda* in sales.
- Canadian drug maker, **Apotex**, is exploring the possibility of a sale, according to sources familiar with the matter. Some major pharmaceutical companies and investors have recently expressed interest. The company is working a financial advisor to review its options that may lead to a partial or full sale of the business, which could fetch as much as US$3 billion. Founded in 1974, Apotex makes generic and innovative drugs and operates in more than 45 countries, including the U.S., Mexico and India.
- **Novartis AG** announced that it has completed its spinoff of its **Alcon** eyecare unit. The transaction was carried out via a dividend-in-kind distribution to Novartis shareholders and American Depository Receipt holders. Each holder received on Alcon share for every five Novartis shares. Novartis emphasized that it is now well-positioned for sustained top- and bottom-line growth, and it plans to improve its innovative medicine core margins into the mid-30s by 2022. Novartis chief executive, *Vas Narasimhan*, said, "We continue to reimagine ourselves as a leading medicines company powered by breakthrough medicines, data science and advanced therapy platforms."
- Pharmaceutical researchers are using big data analysis and machine learning to help find the most appropriate cocktail of drugs to fight cancer. Unlike the cocktail used to fight HIV/AIDS, the possible combinations of drugs number in the millions when fighting different kinds of cancer cells. There are over 300 approved cancer drugs, with thousands awaiting approval that can be combined to target as many as 4.5 million cancer-coding gene mutations that have been identified, making big data and machine learning are valuable tools in narrowing down promising targets.

(Sources: Company Press Releases, Drug Store News, FiercePharma, MarketWatch, Pharma Japan, South China Morning Post)