FDA APPROVAL IS NOT THE ONLY VACCINE CHALLENGE

Early attack demonstrates need for vigilance as the supply chain ramps up to deliver the COVID-19 vaccine to the people.

December 8, 2020 • Industry Week • Peter Fretty

From its onset, the rapid development, approval, manufacture, distribution and dispensing of a COVID-19 vaccine was sure to be an unprecedented challenge. Unfortunately, the potential for serious physical and cyber security issues further complicates the endeavor.

In addition to the warning issued last week by IBM, INTERPOL recently issued an orange warning around the potential for a wide net of organized crime threats to target the COVID-19 vaccines both physically and online, noting that the pandemic has “already triggered unprecedented opportunistic and predatory criminal behavior.”

Early efforts

Unfortunately, some early attacks on key partners have already been successful. Case in point? Americold, a US-based temperature-controlled storage and distribution provider suffered a cyberattack that impacted its operations.

“The attack on Americold shows that cybercriminals will target anyone they believe they can ransom or extort for money. This attack is particularly concerning, as Americold is one of the organizations that will be involved in distributing the upcoming COVID-19 vaccines,” says Gurucul CEO Saryu Nayyar. “As long as there is little chance of getting caught or being punished, cybercriminals will continue their attacks. But the cybersecurity industry will continue developing improved tools, such as security analytics, to help organizations thwart them.”

Point3 Security Vice President of Strategy Chloe Messdaghi adds,“Once again, we see that companies who don’t consider themselves to be likely targets are the most likely of targets. This is especially unfortunate since Americold has an important role to play in the upcoming distribution of COVID-19 vaccines, in addition to its longstanding role in supporting the food supply chain. Each and every piece of the COVID-19 distribution chain must go through serious risk and cybersecurity audits, as though lives depend on it. Because they will.”

According to Messdaghi, “Human operated ransomware attacks begin with trojans or other exploits against unsophisticated vectors. Once a way in is found, malware is planted and privileges are elevated. These attacks often exfiltrate data before encrypting files and the attacks are drawn out, with months of potential compromise adding to the potential harms that can result,”

she says. “That’s why these types of attacks pose a greater threat than automated attacks such as WannaCry or NotPetya – they’re intentional and secretive. The more that our critical data is protected by zero trust actions, the safer we’ll all be – both day to day and particularly in national mobilization circumstances like the upcoming vaccine distribution.”
According to Bill Conner, CEO at SonicWall, “We have seen nation-state threat actors previously target vaccine research to steal incredibly valuable IP. Now, cybercriminals are opening new cyberattack vectors on global deployment, and recalibrating their attacks to target the ‘cold chain’ — the supply chain that helps deliver COVID-19 vaccines at their required cold temperatures.”

“In this instance, evidence suggests that a nation-state is likely behind these attacks — as has been the case for many other attacks against the healthcare, higher-education and government sectors this year. Successful cybercriminal breaches will give these malicious actors the capabilities to influence or control global healthcare, geopolitics and economies during a time of great need,” says Conner. “The supply chain behind these vaccines is incredibly complex and multi-staged. For cybercriminals, the more complex the supply chain, the more potential access points they have to wreak havoc. Whether it be disrupting the shipping process, shutting down the vast freezers needed to keep vaccines cold or hacking into supply chain systems — the outcome of malicious intrusions can dramatically disrupt the entire distribution process, putting lives and economies at risk.”

SonicWall’s Conner tells IndustryWeek, the outcome of a successful attack on the “cold chain” would allow hackers to steal vaccine IP and/or disrupt the vaccine distribution process. “Since the supply chain is interconnected, an attacker having access to a link in the chain results in a higher risk (with increased credibility) of IP theft. If an attacker were to hack into the refrigeration company responsible for keeping the vaccines at the correct temperatures, that attacker could also attempt to infiltrate upstream or downstream – masking the ability to be detected,” says Conner.

“Companies should recognize that every single player in the complex chain in the vaccine distribution process is equally important – not solely the pharmaceutical company which developed the vaccine. As a result, all organizations should be complying with the warnings and guidance issued by governments around cyberattacks,” says Conner. “Companies should ensure that their employees are vigilant and that their security protocols are in place. Specifically, organizations should be paying close attention to phishing attempts, endpoint security, network segmentation and secure access between organizations.”

According to Nayyar, cold storage and distribution could be considered a specialized part of the warehousing and shipping industry verticals. “They have the same basic need for security, but also have the additional refrigeration infrastructure to protect,” she says. “They need to consider themselves a higher value target and improve their security posture to suit. Improved user education. Better perimeter defenses. On-Premises security to protect their specialized on-site systems. Security analytics and endpoint defenses to protect their systems. Whether they need to employ a dedicated team of their own or rely on an MSSP, the issue is a matter of upping their security game.”

Could blockchain help?

Blockchain technology could prove to be a piece in the puzzle especially for the key distribution partners, by increasing transparency via intricate time tracking, assist in proper data management like material and inventory levels, and specifically for this vaccine, transportation temperature. Relying on blockchain to track products, accurately capture costs, and provide transparency will help manufacturers and retailers manage the overwhelming task of delivering COVID-19 vaccines safely.

And, considering the skepticism amongst sectors of the population, integrity and transparency are crucial. "By leveraging blockchain, pharmaceutical manufacturers can show vaccine suppliers and distributors step-by-step details of the vaccine life cycle as well as provide in-depth records of testing data, in addition to manufacturing, distribution and transportation details," Kevin Beasley, CIO at VAI tells IndustryWeek. "With the use of blockchain, pharma companies and manufacturers are able to easily track vaccine distribution, ensuring vaccines are delivered safely to the end destination when the time comes. With a vaccine as sensitive as this one, using blockchain technology to track and record transactions and touch points is key."

Additionally, blockchain can help eliminate fraudulent products from entering the supply chain, explains Beasley. "The Drug Supply Chain Security Act (DSCSA), first introduced in 2013, is the FDA's attempt to require the serialization and traceability of drugs moving throughout the supply chain to eliminate counterfeit drugs, and in this case, vaccines, he says. "Many companies utilize blockchain as an important tool to meet compliance deadlines, decreasing the risk of fraudulent products on the market."
In addition to blockchain, many manufacturers and distributors already have artificial intelligence (AI) in place to increase operations and collect and analyze data to inform things like proper storage, shipping timeliness, and compliance deadlines, so they're used to technology in the supply chain. By adding blockchain, distributors can reap the benefits of using both technologies. "One step further, AI coupled with blockchain can help to prevent recalls - saving money that is often spent fixing problems, having to dispose of dead material, or keeping people from a vaccine even longer," says Beasley.

Road ahead

This could prove to be a pivotal moment for blockchain technology. For instance, beyond pharmaceutical, food manufacturers can implement blockchain to prevent and manage product recalls. "Blockchain has the ability to timestamp data to capture important data points at every step of the food supply chain, which greatly improves the capabilities of companies to track and trace products," says Beasley.

"This allows the company access to an accurate picture of the product's life cycle. With a blockchain system, the food industry would have visibility into data such as product origins, storage temperatures, and ingredients, which helps ensure safety and quality is maintained for end consumers," he says. "Better product visibility would also increase efficiency by avoiding recalls and provide more transparency for customers who want to know where their food comes from."