



OCTOBER 2021

SAFEGUARDING THE COVID-19 VACCINE:

A Case Study in Global Supply Chain Security

Authored By:

Drew Spaniel, Lead Researcher, ICIT

Contributor:

Itzik Kotler, Co-Founder & CTO, SafeBreach

Introduction

CISA has been watching active threats against the coronavirus response since the pandemic started. Initially, the agency focused its efforts on hackers' early targets: top pharmaceutical companies, research organizations, and several dozen companies that supported their functions. Now CISA is working to provide guidance about cybersecurity and physical threats to a wide range of organizations with vastly differing levels of security. Because vaccine distribution protocols vary from state to state, CISA's playbook is always evolving with changes in those procedures, says Corman.

The Biden administration called for the Office of the Director of National Intelligence to assess "ongoing cyber threats and foreign interference campaigns targeting COVID-19 vaccines and related public health efforts." ODNI added, "The DNI is committed to providing the [intelligence community's] best insights and support to policymakers and the nation on this issue."

Cyberattacks by foreign adversaries early in the pandemic focused on espionage and the theft of research. The United States called out both China and Russia over the summer for trying to steal coronavirus research. Those efforts will continue as vaccine makers develop new versions of their drugs. But now added to the mix are attacks against the supply chain seeking to incite U.S. economic and sociopolitical instability.

The European Medicines Agency reported that a hack of documents related to the pandemic led to manipulated and out of context versions of the documents being shared "in a way which could undermine trust in vaccines." In a statement, the EMA said, "The ongoing investigation of the cyberattack on EMA revealed that some of the unlawfully accessed documents related to COVID-19 medicines and vaccines belonging to third parties have been leaked on the internet. Necessary action is being taken by the law enforcement authorities," Cyber-attacks against the U.S. supply chain could have similar results.

- The Pharma industry has lost \$14 billion through Intellectual Property (IP) cyber theft worldwide, according to the United Kingdom Office of Cyber Security and Information Assurance.
- 53% of pharmaceutical IP thefts and related breaches are carried out by bad actors with insider access according to the United Kingdom Office of Cyber Security and Information Assurance.
- The pharma industry's average total cost of a data breach is \$5.06 million, with one of the highest costs of remediating the breach at \$10.81 million across all industries, according to a recent ProofPoint study.
- Over 93% of healthcare organizations experienced a data breach in the past three years and 57% have had more than five data breaches, according to the Cybersecurity Ventures 2020 Healthcare Cybersecurity Report.

Pharmaceutical companies need to protect the COVID-19 vaccine IP, supporting data and supply chains from cyberattacks. The IP behind Covid-19 vaccines and their supporting supply chains needs bleeding edge cybersecurity comprised of holistic technologies and systems, as the vaccines' IP is an asset that cyber attackers have already tried to obtain.

Vaccine Supply Chain Threat Landscape Emphasize the Need for Cybersecurity

In the race to create a Covid-19 vaccine by collaborating across the industry, pharmaceutical companies have exposed more threat surfaces than existed before the pandemic. In R&D, Clinical Trials, Manufacturing and Distribution, there's a proliferation of new threat surfaces cyber attackers are targeting today, as evidenced by threat analysis reports from the U.S. Homeland Security Department's Cybersecurity & Infrastructure Security Agency (CISA).

The report provides specifics about how cyber attackers impersonated an executive from a biomedical company known for having end-to-end cold chain expertise, which is essential for delivering vaccines reliably. The cyber attackers conducted spear-phishing attacks against global companies who support the global cold chain needed for distributing vaccines. There were credential harvesting attempts against global organizations in at least six countries known today to access vaccine transport and distribution sensitive information.

Launching a phishing campaign with the goal of harvesting details on key executives and access credentials across the cold chain is just the beginning. According to Lookout's Pharmaceutical Industry Threat Report, some of the most significant threat surfaces are the most problematic today, including the following:

Research & Development & Clinical Trials

- Collaborative research teams across pharmaceutical manufacturers globally
- Scientists creating initial compounds and completing primary research to define a vaccine
- Integration of study sites at the test device and reporting system level

Manufacturing and Distribution

- Plant workers' systems, including tablets with build instructions on them
- Physician & Pharmacist Networks
- Chemical and Pharmaceutical facilities

Distribution

- Cold storage and vaccine stockpiling systems
- Distribution Channels and their supporting IT systems
- Transport systems
- International efforts

Cyber attackers are taking a more synchronized, multifaceted approach to attacking Covid-19 supply chains, reiterated in CISA's report. There's evidence that state-sponsored cyber attackers are attempting to move laterally through networks and remain there in stealth, allowing them to conduct cyber espionage and collect additional confidential information from victim environments for future

operations. Cyber attackers are initially focused on phishing, followed by malware distribution, registration of new Covid-specific domain names and always looking for unprotected threat surfaces.

Ways Covid-19 Vaccine Supply Chains Need to be Secured

By combining multiple cybersecurity best practices and strategies, pharmaceutical companies stand a better chance of protecting their valuable IP and vaccines. Presented below are ten ways the pharmaceutical industry needs to protect the Covid-19 vaccine supply chain:

Prioritize Privileged Access Management (PAM)

Prioritize Privileged Access Management (PAM) across the vaccine supply chain, ensuring least privilege access to sensitive data starting with IP. CISA's note finds that there have been multiple attempts at capturing privileged credentials, which often have broad access privileges and are frequently left standing open. PAM is needed immediately to institute greater controls around these privileged accounts across the supply chain and only grant just enough, just-in-time access to sensitive IP, shipping and logistics data, vaccination schedules and more. Of the many vendors who compete in this market, Centrify is noteworthy for cloud-based PAM implementations at the enterprise and supply chain level.

Mandate Supply Chain Security

Assess every supplier's security readiness in vaccine supply chains, defining minimum levels of compliance to security standards that include a single, unified security model across all companies. In creating a secured vaccine supply chain, it's imperative to have every supplier network member on the same security model. Taking this step ensures accountability, greater clarity of roles and responsibilities and a common definition of privileged roles and access privileges.

Adopt Zero Trust Frameworks

Taking a Zero Trust-based approach to secure every endpoint across the vaccine manufacturer's R&D, Clinical Trials, Manufacturing and Distribution networks are necessary to shut down cyber attackers taking advantage of legacy security weaknesses approaches. The pharmaceutical companies and myriad logistics providers see a much faster than the expected proliferation of endpoints today. Trusted and untrusted domains from legacy server operating systems are a time sink when it comes to securing endpoints – and proving unreliable despite the best efforts that Security Operations teams are putting into them. Worst of all, they leave vaccine supply chains vulnerable because they often take an outdated “trust but verify” cybersecurity approach.

Segment Networks and Limit Privileges

Extend the Zero Trust framework across the entire supply chain by implementing microsegmentation and endpoint security requirements across all phases of the vaccine's development cycles. This will ensure cyber attackers don't have the opportunity to embed code to activate later. The goal is to push Zero Trust principles to all related processes integrating with the vaccines' pipeline, including all dependencies across the entire development lifecycle.

Require Multi-Factor Authentication

Incorporating Multi-Factor Authentication (MFA) across every system in the vaccine supply chain is a given. Usernames and passwords alone are not enough and MFA is low hanging fruit to authenticate authorized users. MFA is based on two or more factors that can authenticate who you are based on something you know (passwords, PINs, code works), something you have (a smartphone, tokens devices that produce pins or pre-defined pins), or something you are (biometrics, facial recognition, fingerprints, iris and face scans).

“Sell” The Importance of Supply Chain Security to the C-Level

Alleviate the conflicts of who will pay for increasing cybersecurity measures by making supplier-level security a separate line item in any CISOs and CIO's budget. Today certain pharma supply chain CISOs are expected to ramp up cybersecurity programs with the same budget before Covid-19. While there are slight increases in cybersecurity budget levels, it's often not enough to cover the higher costs of securing a broader scope of supply chain operations. CISOs need to have greater control over cybersecurity budgets to protect vaccine IP and distribution. Relying on traditional IT budgets controlled by CIOs isn't working. There needs to be a new level of financial commitment to securing vaccine supply chains. Consider using an AI Ops platform adept at unifying diverse IT environments into a single, cohesive AI-based intelligence system that can identify anomalous network behavior in real-time and take action to avert breaches.

Simplify Network Security with UEM

Unified Endpoint Security (UES) needs to become a standard across all vaccine supply chains now. Vendors who can rapidly process large amounts of data to detect previously unknown threats are needed today to stop cyberattacks from capturing IP, shipment data and valuable logistics information. Pharma supply chains need to have a strategy for achieving more consistent Unified Endpoint Management (UEM) across every device and threat surface of the vaccine supply chain. UEM's many benefits, including streamlining continuous OS updates across multiple mobile platforms, enabling device management regardless of the connection and having an architecture capable of supporting a wide range of devices and operating systems. Another major benefit enterprises mention is automating Internet-based patching, policy, configuration management.

Monitor Cyber and Physical Security Controls

Track-and-traceability is essential in any vaccine supply chain, making the idea of cyber-physical passports that include serialization for vaccine batches more realistic given how complex supply chains are today. Passports are an advanced labeling technology that provides the benefits of virtual tracking, verification of specific compounds and yield rates of key materials. Serialization is a must-have for ensuring greater traceability across vaccine supply chains proving effective in stopping counterfeiting. Having digital passports traceable electronically can further help thwart cyber attackers.

Who is Stealing Our Healthcare Intellectual Property?

Organizations involved in healthcare research and development – including treatments, medical devices, biotechnology, or other subsets of the industry - have valuable IP that is a driver for cybercriminals, economic espionage, and nation-state threats. Cybercriminals seek to exfiltrate personally identifiable information (PII) and protected health information (PHI); disruptive threats like ransomware hold irreplaceable systems, devices, and data sets hostage; and nation states carry out intrusions to steal valuable research and mass records for intelligence gathering purposes. For instance, China's strategic "Made in China 2025" plan pushes for increased domestic development of medical technologies and devices, which may drive threat activity against IP holders and producers of these technologies [7].

FireEye also attributes a growing rise of healthcare research thefts by Chinese advanced persistent threats (APTs) to China's concern over rising cancer rates, their lucrative domestic pharmaceutical market, and their pursuit of cost-effective universal healthcare. Targeting medical research and data from studies may enable Chinese corporations to bring new drugs to market faster than Western competitors, more rapidly develop innovative procedures, and capture geopolitical and market advantages in the global healthcare sector. According to Fire Eye, between 2018 and 2019 there were multiple attacks on research organizations from the Chinese-sponsored APT22, APT41, APT10, and APT18; Russian-sponsored APT28, APT29, and CyberBerkut; and the Vietnamese-sponsored APT32 [7].

Cyber threats on health care facilities can be divided into two categories: targeted and untargeted attacks [7]. Targeted attacks, often launched by insider threats or nation-state APTs, compromise strategic assets in order to achieve engineered outcomes. In contrast, untargeted attacks do not discriminate between assets and opportunistically compromise vulnerable devices. These are typically cybercriminal attacks motivated by short-term financial gains.

Independent Security Evaluators (ISE) identified the most likely adversaries faced by healthcare facilities. According to the report, "a small healthcare facility in an unpopulated area may not be concerned with nation-state or terrorist threats, while a metropolitan area hospital could be." Understanding the profile, motivation, and sophistication of adversaries is paramount to understanding the varying levels of threat actors, their capabilities, and their behavioral patterns [7]. The following high-level overview describes the most likely adversaries faced by healthcare facilities as well as their intentions regarding key assets:

- **Nation-state attackers** are the most likely to inflict long-term impacts on a healthcare research environment through sustained malware infections, the theft of valuable IP, the sabotage of research, and other targeted outcomes that the nation-state sponsor can leverage for economic or geopolitical capital. In some instances, such as the Chinese-sponsored Deep Panda attacks, an APT may target electronic health record databases to either facilitate future campaigns or for the operational insights that can be gleaned when datasets are subjected to machine-learning algorithms. These insights can lead to research, marketing, and other competitive advantages that can be realized on a global scale.
- **Criminal organizations** are motivated by immediate financial gain. Ransomware, the theft of sensitive research, or access-as-a-service operations are the most likely short-term impacts inflicted on healthcare research organizations by cybercriminals. In addition, because of the lack of efficient security controls in many healthcare organizations, the infection of an organization's

network and assets makes it easy to launch distributed attacks on other locations via lateral compromises or botnets.

- **Other Threats Include:**

- Insider threats are motivated by damaging the organization, stealing its research, or harming the public.
- Cyberespionage actors sabotage research based on fiscal, ideological, or geopolitical motivations.
- Individuals and small hacker collectives may be motivated by profit and notoriety.
- Hacktivists are motivated by political and financial gain, most often seeking to embarrass, discredit, blackmail, or sell information about high profile individuals.
- Terrorists are motivated by inspiring fear and causing harm.

Conclusion

By closing the cybersecurity gaps in vaccine supply chains, the world's nations can find new, leaner, more efficient processes to distribute vaccines and protect their citizens. It's evident from the results achieved so far in the U.S. alone that relying on traditional supply chains and means of distribution isn't getting the job done fast enough and cyber attackers are already looking to take advantage. By combining multiple cybersecurity tactics, techniques and procedures, the vaccine supply chain stands to improve and be more secure from threats.