BLUE GLACIER

Blue Glacier Red Team

A Red Team Special Memorandum **July 30, 2021**

This memo was prepared by Blue Glacier Security & Intelligence® to provide a pronounced "out-of-the-box" approach that will provoke thought and offer an alternative viewpoint on analytic issues. Comments and queries are welcome and may be directed to Blue Glacier at 703-934-2034 or 202-389-6200.

Dangers at the Intersection of Cybercrime, Pandemic Fatigue, and Anti-Vaccination Militancy

The COVID-19 vaccine is one of the primary tools used to achieve herd immunity and subsequently end the pandemic. Rollout occurs in three main stages: production, distribution, and administration. Each stage has cyber vulnerabilities. Motivated by anti-vaccination conspiracy theories or animosity towards pandemic-related restrictions, hacktivists might attack the vaccine chain, attempt to manipulate medical records, or distort critical COVID-19 surveillance data. These attacks could disrupt vaccination efforts.

Vaccination Disruptions Could Delay Herd Immunity

The U.S. Centers for Disease Control and Prevention (CDC) highlights the role of vaccines in reaching herd immunity and ending the COVID-19 pandemic.[1] Johns Hopkins University projects that a given population will need to hit at least 70% vaccinated to achieve herd immunity.[2] Delays in vaccinations could slow progress towards the 70% benchmark. In order to safeguard public health efforts, officials should be aware of vulnerabilities in vaccine infrastructure and the potential cyber threats posed by extremists—particularly those in the anti-vaccination ("anti-vax") movement. Some anti-vaxxers believe vaccinations are linked to serious medical side effects, such as autism in young children.[3]

Precedence for Cyber Attacks Against COVID-19 Vaccine Infrastructure

Healthcare is one of the most targeted sectors for cybercrime,[4] and the COVID-19 vaccine rollout is no exception. Hackers have repeatedly targeted vaccine-related research and the COVID-19 cold chain. The cold chain ensures vaccines remain at the proper temperature during storage and transport. Throughout 2020 the cyber espionage group Advanced Persistent Threat 29 (also known as "the Dukes", "Cozy Bear", or "YTTRIUM"), almost certainly part of the Russian intelligence services, attempted to steal vaccine research from Canadian, British, and American companies.[5] Those responsible for attacking the cold chain remain unknown. Hackers have repeatedly tried to infiltrate members of the cold chain using spear-phishing email operations. According to IBM Security, 44 separate cold chain partner organizations across 14 countries have reported cyberattacks. Targets include research firms, government agencies, medical manufacturers, pharmaceutical companies, immunology experts, and pharmacies.[6]

Potential Motives for Attacking Vaccine Rollout

Motives to attack vaccine infrastructure could include monetary gain, anti-vaccination militancy, vaccine-related nationalism, pandemic fatigue, or a combination thereof. The World Health Organization defines pandemic fatigue as "demotivation to follow recommended protective behaviors, emerging gradually over time and affected by a number of emotions, experiences and perceptions."[7]

Militant anti-vaxxers, particularly those spurred on by "plandemic" or "scamdemic" conspiracy theories, might be most interested in disrupting vaccine injections.

- In April 2021, anti-vax extremists firebombed a COVID-19 vaccination center in Brescia, Italy. Assailants reportedly belonged to the online "No Vax" movement.[8]
- A Los Angeles COVID-19 vaccination site—one of the largest in the U.S.—was temporarily shut down in January 2021 after anti-vax protestors obstructed the entrance.[9]

Individuals convinced that the pandemic was planned or a scam likely regard medical COVID-related data as false, and might view manipulating it as a fight against government conspiracy. Those motivated by pandemic fatigue could target vaccine production, distribution, or administration as a form of protesting pandemic-related restrictions.

- In March 2021, protests against pandemic-related restrictions turned violent across Europe, with police forcibly clearing protestors in Germany and the United Kingdom.[10] Similar protests occurred in Austria, Finland, Romania, Switzerland, Poland, France, Bulgaria, Serbia, the Netherlands and Romania.[11]

Potential Structure of Anti-Vaccination Hacking Teams

Cybercriminals who attack vaccine infrastructure could operate in groups or as lone actors. Precedence exists for cybercrime groups living in and coordinating from several different nations, such as the “Anonymous” hacktivist collective.[12] Anonymous consists of a loose international network of cyber activists united around certain shared principles. Supporters of far-right conspiracy theory movements such as QAnon[13] could adopt a structure similar to Anonymous in carrying out anti-vax attacks. QAnon has been quick to accept members of the anti-vax movement into its ranks as “COVID-19 anti-vax narratives fit squarely into the QAnon playbook by playing on the distrust of authority.”[14]

- In April 2020, far-right conspiracy theorists stole and published over 25,000 email addresses related to organizations fighting the COVID-19 pandemic. The hackers called for a harassment campaign, citing pandemic-related conspiracy theories as justification.[15]

Production

Risks to Vaccine Factories

Two widely used U.S. vaccines are produced domestically by Pfizer and Moderna. Pfizer bottles vaccines in Pleasant Prairie, Wisconsin and Kalamazoo, Michigan.[16]

The majority of Moderna vaccines are bottled in Norwood, Massachusetts.[17] These factories could be targeted by cybercriminals. For example, if factory temperature controls are compromised by a cyberattack, a large number of vaccines might spoil.

- COVID-19 vaccines require strict temperature controls to keep from spoiling. The Pfizer vaccine must be kept between -112°F and -76°F until arriving at the vaccination center.[18] The Moderna vaccine must be kept between -58°F and 5°F.[19]

Hackers could attempt to disrupt power to the production facilities, thus disabling the vaccine refrigeration system. Hackers might also attempt to change thermometer settings if refrigerators are networked.

Distribution

Hackers Could Target Shipping Companies

The three vaccine production facilities transport the vaccine vials to nearby airports. Shipping giants UPS and FedEx act as the primary national distributors of COVID-19 vaccines.[20] Hackers might manipulate or delete data from carriers' inventory management systems, leading to disruptions in vaccine shipments. Cyberattacks could also target systems used to upload flight plans into the aircraft. These attacks could temporarily ground portions of each carrier's fleet and cause delays. Attacks against carriers need not target shipping directly to disrupt vaccine distribution. Hackers could attack other business segments and then demand a halt to vaccination delivery.

- A FedEx subsidiary was "significantly affected" by an information system virus in June 2017. Hackers targeted the carrier's operations and communications systems, disrupting service and delaying shipments.[21] The malware might have been a modified version of the Petya virus, a notorious strain of ransomware.[22]

- In June 2015, a cyberattack jammed LOT Polish Airline's computer systems.[23] The distributed denial of service attack lasted 5 hours and froze systems responsible for uploading flight plans before takeoff. Ten flights were cancelled and 15 were delayed by the attack.[24]

Administration

State and Federal Databases are Vulnerable to Cyberattacks

Vaccination rollout in the United States is more decentralized than in many other nations. A combination of federal and state-based systems coordinates vaccine administration. Main programs at the federal level include the Vaccine Tracking System (VTrckS), Vaccine Administration Management System (VAMS), and the Tiberius database.[25] VTrckS allows local health departments to monitor vaccine locations. An attack on VTrckS could manipulate tracking data and lead states to misallocate vaccines between storage and administration sites. VAMS is an optional federal system for states to organize vaccination appointment scheduling. By disabling VAMS, hackers could disrupt vaccination appointments in some states. States primarily use the Tiberius database to track vaccine allotment from the federal government and to create local vaccine distribution strategies. A cyberattack on Tiberius could disrupt state-wide vaccination planning.

States use individual registries to compile immunization information and order vaccines. Hackers could corrupt, manipulate, or steal immunization records from one or more state databases. Disabled state registries could lead to vaccination delays. Additionally, stolen medical information is in high demand on the dark web.[26] Leaked immunization records containing protected health information (PHI)[27] could lead to identity theft.[28]

Social Media as a Tool for Hacking and Disruption

Using social media, cybercriminals could find personal information about public health officials and employees working within the vaccine infrastructure. Hackers could then conduct spear-phishing to steal login credentials or place malware on company systems.

- In September 2020, hackers launched an email phishing campaign impersonating a Haier Biomedical executive. The emails targeted organizations involved in COVID-19 cold chain transportation. IBM Security concluded the attackers likely sought to harvest credentials for future access to sensitive vaccine rollout information.[29]

The Biden Administration plans to launch door-to-door vaccination information teams during summer 2021. Anti-vax militants could use social media to threaten or coordinate harassment and attacks on the teams. Militants might prefer applications with less stringent content standards—such as Parler or MeWe.

- Extremists coordinated the January 6th attempted insurgency at the U.S. Capitol largely through social media. Top sites included Facebook, Twitter, Parler, and MeWe.[30]
- A recent Morning Consult poll found that 39% of all registered voters oppose door-to-door vaccination teams. [31] Criticism of the teams featured volatile rhetoric. The governor of Missouri falsely claimed that federal "agents" were being sent to "compel vaccination."[32]
- A May 2020 county supervisors meeting in California was attended by people opposed to an order requiring face coverings. One attendee read aloud the home address of the order's author, county Chief Health Officer Dr. Nichole Quick, as well as the name of her boyfriend. Quick had previously received several threatening statements both in public comment and online. Reportedly about 80% of local health directors across California said they or their personal property had been threatened since the pandemic began.[33]
- In August 2019, California State Senator Richard Pan was assaulted by an anti-vax extremist.[34] The attack was in response to Senator Pan introducing Senate Bill 276—legislation aimed at strengthening state vaccination requirements.[35] The bill passed the following month, prompting an anti-vax demonstrator to throw red liquid onto the senate floor.[36]

Black Market Use of Stolen Vaccine Data

Black marketeers could use stolen lot numbers to produce fake vaccination cards. With no unified federal database for tracking immunizations, proof of vaccination in the U.S. is largely based on an honor system. COVID-19 vaccination cards are only sheets of paper inscribed with a patient name, vaccination date, and vaccine lot number.[37]

- In May 2021, a restaurant owner in San Joaquin County, California was arrested for selling fake vaccination cards at $20 apiece.[38]
- In July 2021, authorities charged a naturopathic doctor in Napa, California after she made over $7,000 from fake vaccination cards and "immunization pellet" treatments.[39]
- Fake COVID-19 vaccine "passports" for multiple countries are available on the dark web. Costs range from $100 to $200 per passport.[40]

If hackers release stolen vaccine lot numbers on the dark web, authorities and companies might have difficulty differentiating between authentic and fraudulent vaccine cards. Schools, businesses, and similar entities would temporarily be unable to verify if their employees are vaccinated. Many organizations plan to require proof of vaccination before allowing employees back into the office.

- According to a University of Arizona study, 60% of employers—including schools and government agencies—will require employees to demonstrate proof of vaccination against COVID-19 before allowing them to return to work.[41]

[1] "COVID-19: Key Things to Know." Centers for Disease Control and Prevention. (June 2021). https://www.cdc.gov/coronavirus/2019-ncov/vaccines/keythingstoknow.html

[2] D'Souza, Gypsyamber and David Dowdy. "What is Herd Immunity and How Can We Achieve It With COVID-19?" Johns Hopkins Bloomberg School of Public Health. (Apr 2021). https://www.jhsph.edu/covid-19/articles/achieving-herd-immunity-with-covid19.html

[3] Hussain, A., Ali, S., Ahmed, M., & Hussain, S. "The Anti-vaccination Movement: A Regression in Modern Medicine." (July 2018). https://doi.org/10.7759/cureus.2919

[4] "Cyber Security in Healthcare." Osterman Research White Paper. (Feb 2020). https://cdn.www.carbonblack.com/wp-content/uploads/VMWCB-Report-Cyber-Security-in-Healthcare.pdf

[5] "Advisory: APT29 targets COVID-19 vaccine development." National Cyber Security Centre. (July 2020). https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF

[6] Frydrych, Melissa and Claire Zaboeva. "An Update: The COVID-19 Vaccine's Global Cold Chain Continues to Be a Target." IBM Security. (Apr 2021). https://securityintelligence.com/posts/covid-19-vaccine-global-cold-chain-security/

[7] "Pandemic Fatigue: Reinvigorating the public to prevent COVID-19." World Health Organization. (2020). https://apps.who.int/iris/bitstream/handle/10665/335820/WHO-EURO-2020-1160-40906-55390-eng.pdf

[8] "Brescia vaccine centre arson: Italian police arrest two anti-vaxxers for Molotov cocktail attack." Euronews. (May 2021). https://www.euronews.com/2021/05/03/italian-police-arrest-two-anti-vaxxers-for-brescia-vaccine-centre-arson-attack

[9] "Anti-vaccine protesters temporarily shut down vaccine site." ABC News. (Jan 2021). https://abcnews.go.com/Health/wireStory/anti-vaccine-protesters-temporarily-shut-vaccine-site-75586520

[10] McCarthy, Julie. "Protesters Across Europe Clash With Police Over COVID-19 Lockdowns." NPR. (Mar 2021). https://www.npr.org/2021/03/21/979653125/protesters-across-europe-clash-with-police-over-covid-19-lockdowns

[11] Dettmer, Jamie. "Lockdown Protests Snowball as Europe's Libertarians Fret About Freedom." Voice of America. (Apr 2021). https://www.voanews.com/covid-19-pandemic/lockdown-protests-snowball-europes-libertarians-fret-about-freedom

[12] Sands, Geneva. "What to Know About the Worldwide Hacker Group 'Anonymous'." ABC News. (Mar 2016). https://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302

[13] "Factbox: What is QAnon and how are online platforms taking action on it?" Reuters. (Sept 2020). https://www.reuters.com/article/us-socialmedia-qanon-factbox/factbox-what-is-qanon-and-how-are-online-platforms-taking-action-on-it-idUSKBN26203M

[14] Kovalcikova, Nad'a and Caitlyn Ramsey. "QAnon and Anti-Vax Conspiracy Theories Pose a Threat to Democracy Beyond National Borders." Alliance for Securing Democracy. (Mar 2021). https://securingdemocracy.gmfus.org/qanon-and-anti-vax-conspiracy-theories-pose-a-threat-to-democracy-beyond-national-borders/

[15] Schwartz, Kenneth. "Far-Right Extremists Publish 25,000 Email Addresses Allegedly Tied to COVID Fight." Voice of America News. (Apr 2020). https://www.voanews.com/covid-19-pandemic/far-right-extremists-publish-25000-email-addresses-allegedly-tied-covid-fight

[16] "Manufacturing and Distributing the COVID-19 Vaccine." Pfizer. https://www.pfizer.com/science/coronavirus/vaccine/manufacturing-and-distribution

[17] "Moderna to Expand Norwood Plant to Boost COVID Vaccine Production." NBC10 Boston News. (May 2021). https://www.nbcboston.com/news/coronavirus/moderna-to-expand-norwood-plant-to-boost-covid-vaccine-production/2371508/

[18] "Pfizer-BioNTech COVID-19 Vaccine Storage and Handling Summary." Centers for Disease Control and Prevention. https://www.cdc.gov/vaccines/covid-19/info-by-product/pfizer/downloads/storage-summary.pdf

[19] "Moderna COVID-19 Vaccine Storage and Handling Summary." Centers for Disease Control and Prevention. (July 2021). https://www.cdc.gov/vaccines/covid-19/info-by-product/moderna/downloads/storage-summary.pdf

[20] Wooddell, Brody. "UPS and FedEx set to deliver COVID vaccines per White House mandate." ABC News. (Dec 2020). https://www.abcactionnews.com/news/coronavirus/ups-and-fedex-set-to-deliver-covid-vaccines-per-white-house-mandate

[21] "TNT Express Operations Disrupted, All Other FedEx Services Operating Normally." FedEx Investor Relations. (June 2017). https://investors.fedex.com/news-and-events/investor-news/investor-news-details/2017/TNT-Express-Operations-Disrupted-All-Other-FedEx-Services-Operating-Normally/default.aspx

[22] O'Kane, Sean. "FedEx's Dutch operations have been 'significantly affected' by the Petya virus." The Verge. (June 2017). https://www.theverge.com/2017/6/28/15887726/fedex-tnt-express-petya-virus-spread

[23] "Today afternoon LOT Encountered IT Attack, That Affected Our Ground Operations Systems." Corporate Press Releases. LOT Polish Airlines. (June 2015). https://corporate.lot.com/pl/en/press-news?article=772922

[24] Kharpal, Arjun. "Hack attack leaves 1,400 airline passengers grounded." CNBC. (June 2015). https://www.cnbc.com/2015/06/22/hack-attack-leaves-1400-passengers-of-polish-airline-lot-grounded.html

[25] "Tracking COVID-19 Vaccines: U.S. Data Systems and Related Issues." Congressional Research Service. (Jan 2021). https://crsreports.congress.gov/product/pdf/IN/IN11584

[26] Farr, Christina. "On the Dark Web, Medical Records Are A Hot Commodity." Fast Company. (July 2016). https://www.fastcompany.com/3061543/on-the-dark-web-medical-records-are-a-hot-commodity

[27] "HIPAA PHI: Definition of PHI and List of 18 Identifiers." Human Research Program. University of California Berkley. https://cphs.berkeley.edu/hipaa/hipaa18.html

[28] "What To Know About Medical Identity Theft." Consumer Information. Federal Trade Commission. https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft

[29] Zaboeva, Claire and Melissa Frydrych. "IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain." IBM Security Intelligence. (Dec 2020). https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/

[30] Atlantic Council's DFRLab. "#StopTheSteal: Timeline of Social Media and Extremist Activities Leading to 1/6 Insurrection." (Feb 2021). https://www.justsecurity.org/74622/stopthesteal-timeline-of-social-media-and-extremist-activities-leading-to-1-6-insurrection/

[31] Galvin, Gaby. "65% of GOP Voters Oppose Biden's Door-to-Door COVID-19 Vaccination Push." The Morning Consult. (July 2021). https://morningconsult.com/2021/07/14/biden-door-to-door-covid-vaccines-white-house-poll/

[32] Parson, Mike. Twitter Post. July 7, 2021, 8:47 PM. https://twitter.com/GovParsonMO/status/1412936318850580481

[33] "Public Health Workers Fighting Virus Face Growing Threats." The Associated Press. (June 2020). https://apnews.com/article/co-state-wire-only-on-ap-health-nc-state-wire-virus-outbreak-8839ed5e94eea718304820218919738e

[34] "'I don't regret pushing him': Man cited for shoving California state senator." KCRA News. (Aug 2019). https://www.kcra.com/article/california-state-senator-richard-pan-assault/28777200

[35] Ho, Vivian. "Lawmaker who faced anti-vax attack: "The movement is growing more violent." The Guardian. (Feb 2021). https://www.theguardian.com/world/2021/feb/03/anti-vaxxers-coronavirus-vaccines-california-richard-pan

[36] Holcombe, Madeline. "Woman is arrested after California lawmakers are splashed with red liquid on Senate floor." CNN. (Sept 2019). https://www.cnn.com/2019/09/14/us/california-senate-red-liquid/index.html

[37] Bogost, Ian. "No One Actually Knows If You're Vaccinated." *The Atlantic.* (May 2021). https://www.theatlantic.com/health/archive/2021/05/america-covid-vaccine-honor-system/618891/

[38] Smith, Haley. "California bar owner charged with selling fake COVID-19 vaccination cards." *Los Angeles Times.* (May 2021). https://www.latimes.com/california/story/2021-05-06/bar-owner-charged-with-selling-fake-covid-19-vaccine-cards

[39] *United States of America v. Juli Mazi.* United States District Court for the Northern District of California. Case No.3:21-mj-71156 MAG. (July 2021). https://sanfrancisco.cbslocal.com/wp-content/uploads/sites/15116056/2021/07/mazi_complaint.pdf

[40] "A passport to freedom? Fake COVID-19 test results and vaccination certificates offered on Darknet and hacking forums." Check Point Software Technologies LTD. (Mar 2021) https://blog.checkpoint.com/2021/03/22/a-passport-to-freedom-fake-covid-19-test-results-and-vaccination-certificates-offered-on-darknet-and-hacking-forums/

[41] L. Wade, Nathaniel and Mara G. Aspinall. "Back to the Workplace: Are we there yet?" Arizona State University, College of Health Solutions. (Apr 2021). https://www.rockefellerfoundation.org/wp-content/uploads/2021/04/ASU-Workplace-Commons-Phase-2-Report-4-28-21.pdf