CYBER
THREAT
ANALYSIS

Recorded Future®

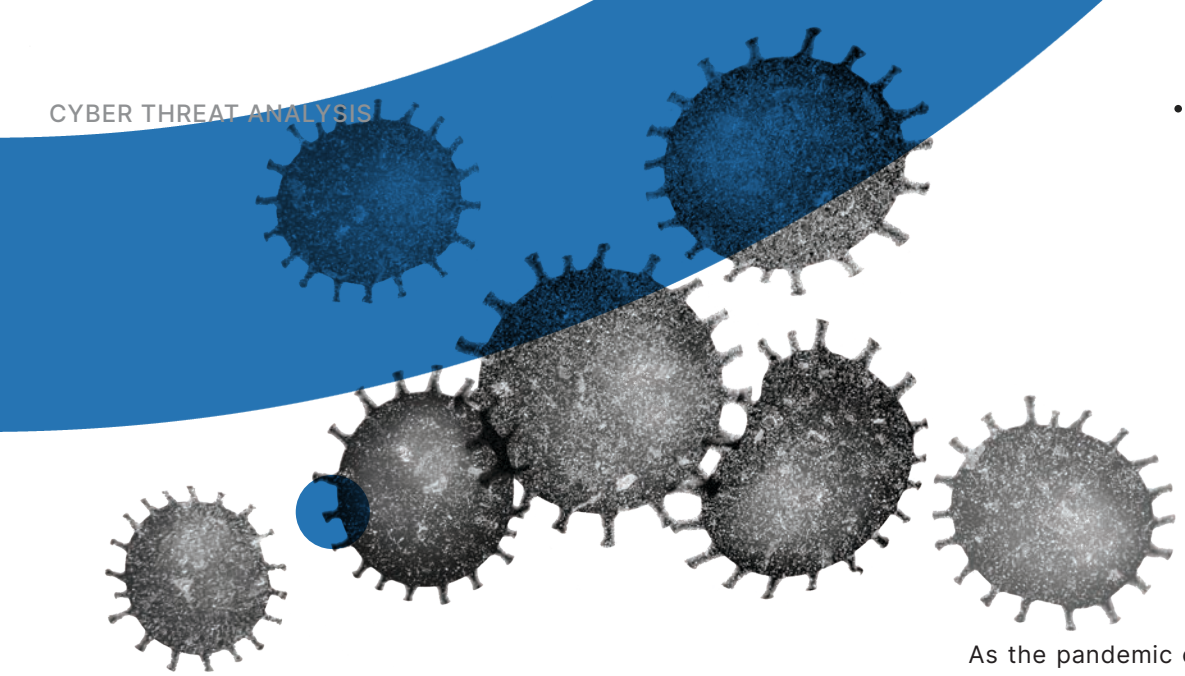
By Insikt Group®

CTA-2021-0122

FOLLOW THE MONEY:

QUALIFYING OPPORTUNISM BEHIND CYBERATTACKS DURING THE COVID-19 PANDEMIC

Recorded Future®



This report covers the cybersecurity threats tied to the COVID-19 pandemic that Recorded Future has observed over the past year, detailing the socioeconomic drivers that contributed to the threat landscape. This research is targeted toward those looking to understand the evolution of the COVID-19 pandemic's effects on the cybersecurity landscape and the opportunism of cybercriminals and nation-state threat actors.

Executive Summary

The COVID-19 pandemic has created significant disruption to the global economy, and the cyber threat landscape has responded accordingly; criminal, extremist, and state-sponsored threat actors have capitalized on the pandemic's worldwide economic crisis. Throughout the pandemic, the tactics used by threat actors have evolved to focus on the most pressing, timely concerns and exploit those public fears and uncertainty that present the greatest opportunity for successful victimization.

Recorded Future correlated aspects of this opportunism with changes in the socioeconomic climate spurred by the different stages of the pandemic, and their resulting effects on organizations and the public. Initially, threat actors largely capitalized on the public's hunger for information about the new virus, and on shortages in personal protective equipment (PPE) and tests. Later, threat actors pivoted to attacks focused on stealing information related to the development of the vaccine, disruption of healthcare providers, and scams targeting financial concerns. Finally, the most recent threat activity shows threat actors pivoting to targeting organizations involved in the development and delivery of the vaccine using disruption and misinformation techniques.

As the pandemic continues, criminals will continue to target organizations focused on the delivery of the vaccine, especially as global distribution increases. Threat actors' tactics will likely evolve to discredit the vaccine's safety and efficacy, or seek to steal information of individuals who have been vaccinated or participated in trials. Finally, competing nation-states will continue to spread false information about COVID-19 in an effort to gain economic advantage over competitors and discredit adversaries.

Key Judgments

- The opportunism of threat actors is primarily created by the socioeconomic conditions of the pandemic and is visible in the evolution of the themes used to target victims over the course of the pandemic.
- Threat actors have targeted the healthcare and vaccine "ecosystems" with a variety of tactics aimed at financial exploitation, intelligence gathering, and destruction.
- China and Russia each conducted coordinated and aggressive disinformation campaigns targeting Western democracies such as the United States and United Kingdom. Manipulating global audiences towards favoring their own systems of governance is a long-term strategic objective of both China and Russia. However, despite similar aims, their influence operations tactics vary based on unique tool sets and resources.
- China and Russia each used information operations to target vaccine developers and the COVID economy in Western nations to gain business and economic advantage over competitors.

Background

Threat actors, both financially motivated and state-sponsored, have taken advantage of different aspects of the pandemic to create thematic lures that entice victims into compromising their systems. These themes include scams around PPE shortages, changes brought on by the move to remote work, COVID testing and tracking, and most recently, vaccine development and the supply chain that supports its delivery. Ultimately, financially motivated threat actors are aiming to maximize profit and as such use tactics aimed at generating the most profit, crafting scams that most effectively play on the fears and concerns of their victims at each stage of the pandemic. Similarly, state-sponsored threat actors have used aspects of the pandemic to further victimize existing adversaries, as well as gain intelligence on scientific developments around vaccine candidates.

At the most basic level, existing businesses have deployed new products and services, including fashion companies marketing their line of masks, advertisement of COVID-19 safety protocols to draw customers, an increase in "virtual" versions of in-person events and seminars, and an increase in the number and types of experiences and products that can be delivered to one's home. More significantly, new products and industries have also emerged, specifically those around COVID-19 diagnostics and testing, "COVID-19 cleaning" services, and the mobilization of a supply chain to bring the vaccine to the public.

The negative economic ramifications of sustained lockdowns have manifested themselves in public concern about foreclosures on homes, loss of business, inconsistent financial relief, lack of access to healthcare services and testing, and uncertainty surrounding how much "normalcy" a vaccine will bring and when. Threat actors and scammers have continued to exploit these fears in a variety of ways, preying on economic hardship and the public's fear to profit financially or further intelligence goals.

Threat Analysis — The COVID Economy

The COVID-19 pandemic has caused stark changes in the world economy, and with it, groups who have benefited financially and those who have not. We have observed threat actors, both nation-state and criminal, take advantage of the pandemic to profit in a variety of ways. To understand what socioeconomic events created opportunities for threat actors to victimize individuals and organizations throughout the world, it is critical to understand the motivations of these threat actors.

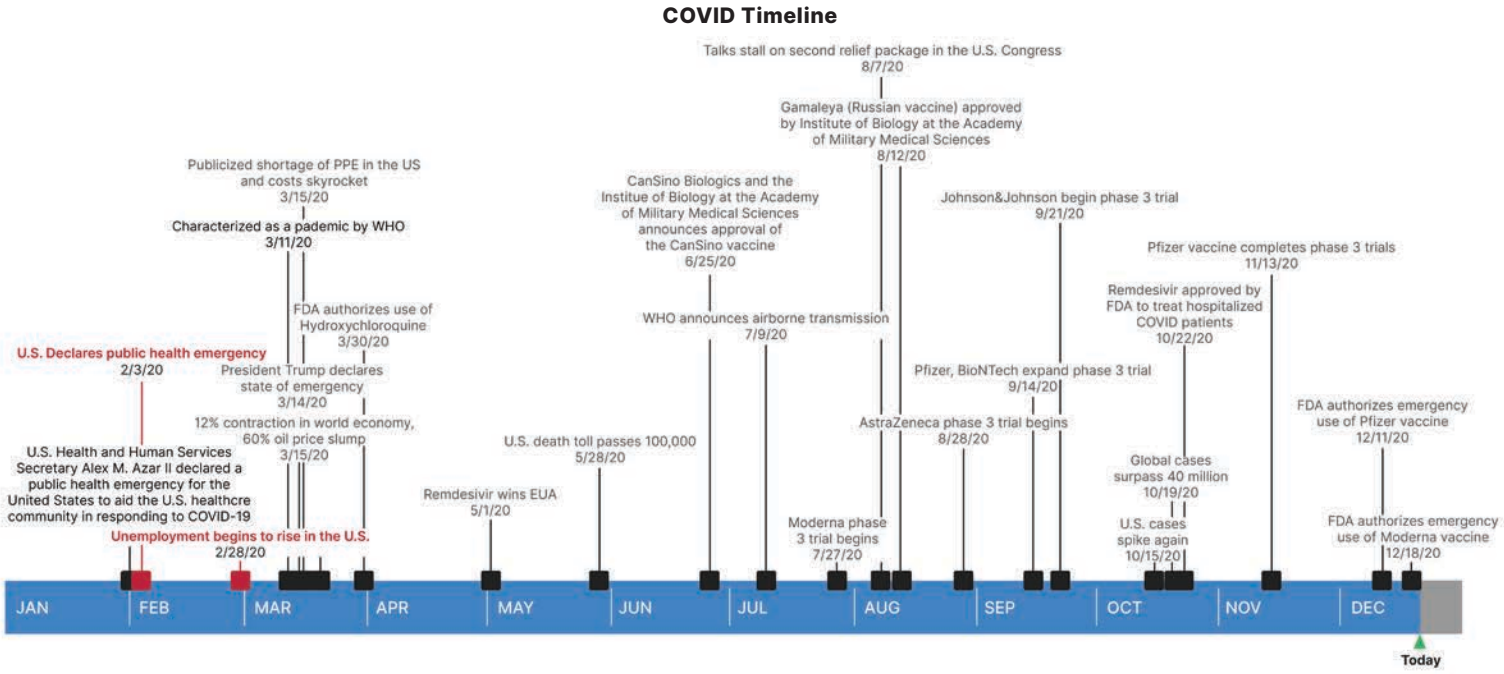


Figure 1: Key events in the COVID-19 pandemic from January 2020 through December 2020

Timeline of The COVID-19 Pandemic

As different nations moved to enact measures to combat the pandemic, and scientific developments on vaccines and treatments moved forward, the secondary effects of these events began to create an economic impact in many different industries and markets. Some of the key events in the pandemic are included in Figure 1 below:

COVID-19 Timeline

In this report, Insikt Group highlights the relationship between these events, key industries involved, and the types of cybersecurity incidents we observed to qualify the opportunism of threat actors and how this opportunism evolved over the course of the last year.

What Motivates Threat Actors?

At a most basic level, cybercriminal threat actors are primarily motivated by financial incentives, and intrusions are driven by the potential for profit. Primarily, we see cybercriminal threat actors employ the following techniques to target victims:

- **Phishing:** Threat actors send victims an email containing a malicious link or attachment that causes the victim to download malware or input credentials. These emails contain "lures" that may impersonate a website login page, a package delivery confirmation, or promise to provide information of interest to the victim. The actor profits only if the victim downloads the malware or clicks on the link, so it is of utmost importance for the threat actor to create an enticing lure.
- **Ransomware:** Ransomware may be delivered by any number of methods, but phishing remains popular. While some ransomware may be deployed opportunistically, researchers have developed models based on game theory that suggest the "attractiveness" of a target depends on a number of factors, including an organization's ability and willingness to pay a ransom demand (as designated by several factors).
- **Scams and Fraud:** Frequently, scams are lower-tech ways criminals target victims, often with the promise of goods or services with the provision of money or personal information required up front. Often, scams are perpetrated through social media, telemarketing calls, text messaging, or even door-to-door visits. Scams may become slightly more "technical" with threat actors offering fake or repackaged commodity tools on dark web technical forums. Again, scams and fraud are only profitable if they succeed in enticing victims.
- **Business Email Compromise (BEC):** Criminals send a message that appears to come from a known source making a legitimate request and this tactic relies primarily on social engineering to be successful. These requests may be for the transfer of funds, payments, or personally identifiable information.

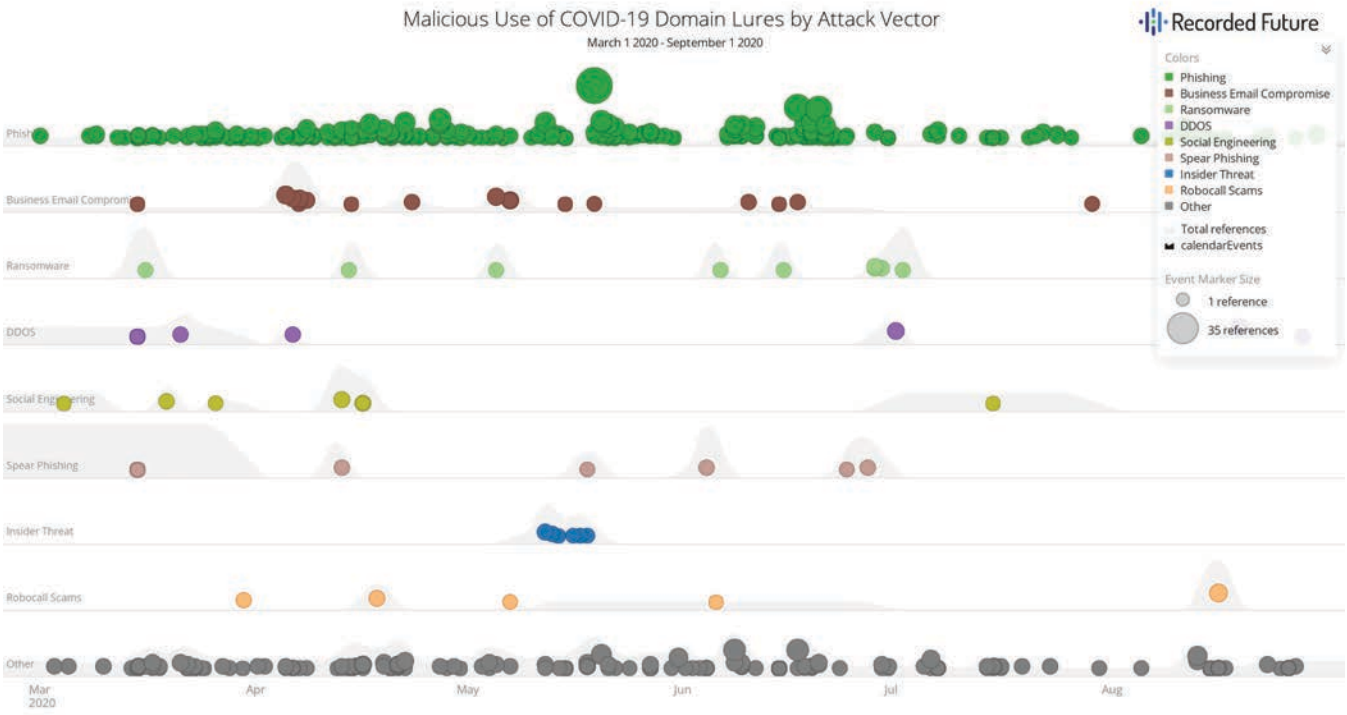


Figure 2: Frequency of use of attack vectors that use COVID-19 domain lures from March 1, 2020 through September 1, 2020

Figure 2, above, shows the use of these and other attack vectors with COVID-19-themed domain lures between March 1 2020 and September 1 2020.

State-sponsored threat actors may be motivated by a variety of factors, though direct financial motivation plays a smaller role than other factors. Some of the key nation-states and their motivators include:

- **China:** The Chinese government's focus throughout the pandemic has been to control the spread of the virus within the country's borders and to counter the narrative that COVID-19 originated in Wuhan. Throughout 2020, the Communist Party of China (CCP) made significant efforts to create the perception that they have the virus under control, that the fallout is minimal, and that the current Chinese mode of governance is more competent than Western models. China's strong response was also likely driven by a need to ensure the continuation of economic growth, from which much of the CCP's political legitimacy is derived. Chinese media have consistently pushed the narrative that China is a capable world power despite the challenges that COVID-19 presented throughout the year. The competition to create the first COVID-19 vaccine, have it approved, and sell it around the world is driving intense espionage campaigns around the world. In May 2020, the U.S. Department of Homeland Security and the FBI issued a joint statement warning that China was conducting cyberespionage operations targeting U.S. research institutions and pharmaceutical companies in an effort to steal proprietary information used to develop a vaccine. In July 2020, the U.S. Department of Justice announced indictments of two Chinese hackers who allegedly work for China's Ministry of State Security, stating that the defendants probed for vulnerabilities in computer networks of companies developing COVID-19 vaccines, testing technology, and treatments.
- **Russia:** Much of the cyberespionage activity linked to Russian state-sponsored threat actors in 2020 has targeted organizations developing COVID-19 vaccines. At the onset of the pandemic, Vladimir Putin retreated to a largely private, protected environment, and put the onus on local governments to manage the pandemic in their respective regions. Russia has begun to deploy the Sputnik V vaccine to its citizens after announcing its availability before fully completing wide-scale trials, with the Gamaleya National Center of Epidemiology and Microbiology claiming a 92% efficacy rate, a claim that is questioned by international researchers. Despite the purported high efficacy rate of Sputnik V, there are indications that Gamaleya is also reaching out to foreign partners for support in improving the vaccine, including the makers of the Oxford/AstraZeneca vaccine. On December 21, 2020, Gamaleya, the Russian Direct Investment Fund (RDIF), and the Russian pharmaceutical company R-Pharm signed a memorandum of cooperation

with pharmaceutical developer AstraZeneca to combat COVID-19. Putin was at his lowest popularity level since the beginning of his presidency at the outset of the pandemic, and by being seen as the driving force in the delivery of the vaccine to his constituents, he can likely increase his popularity and decrease the threat of domestic unrest. Experts suspect that Russia is undercounting their coronavirus death toll, reporting around 6,000 more deaths from all causes in May than the average of the last three years; on December 29, 2020, the Russian state statistics agency Rosstat reported "that the death toll from COVID-19 is more than three times as high as officially reported". With the price of oil fluctuating at or below just over $40 per barrel for most of 2020, combined with economic sanctions imposed by the U.S. and the country's struggles with the virus, Russia is suffering financially, further underscoring the need for the country to successfully combat the virus. There are also indications that Putin is seeking to pivot away from reliance on an oil-based economy, with Russian state-owned media source Tass reporting that the Russian president has declared 2021 to be a "Year of Science and Technology". Putin further emphasized the pivot away from oil in a December 2020 announcement, stating, "If someone wants to still view us as a gas station, well that image is no longer valid." At the same time, the president acknowledged that "the dependence [on oil and gas revenues] is still very large," and this factor must be taken into account.

- **North Korea:** North Korea is one of the most closed-off countries in the world, but smuggling activity, which is common through the Northern border with China, creates a vulnerability to COVID-19 infection. However, Kim Jong-un has repeatedly stated that there has been no outbreak in his country and brags that the Democratic People's Republic of Korea is a "shining success" in the fight against COVID-19. Experts believe that North Korea would be particularly vulnerable to the pandemic if widespread infection were to occur because its healthcare infrastructure would be ill-equipped to handle large numbers of critically ill patients. However, North Korea is uniquely positioned to minimize the community spread of COVID-19 for a couple of key reasons: one, the borders are largely closed off and cross-border travel is strictly limited to essential personnel; and two, citizens within its borders are severely limited in their ability to travel and move about the country unchecked. Despite claims that North Korea has been completely COVID-free, alleged North Korean hackers targeted the computer networks of at least three vaccine development companies.

Exploiting the Economic Effects of COVID-19

Insikt Group observed malicious activity targeting several aspects of the COVID-19 pandemic and organizations economically impacted by it. This malicious activity included phishing schemes, fraud, and scams capitalizing on aspects of the pandemic, the exploitation of organizations involved in healthcare and the development or delivery of the vaccine, registration of domains that used COVID-19-related terms or themes maliciously, and disinformation campaigns seeking to confuse the public and control the narrative for financial, political, or ideological gain.

Domain Registrations

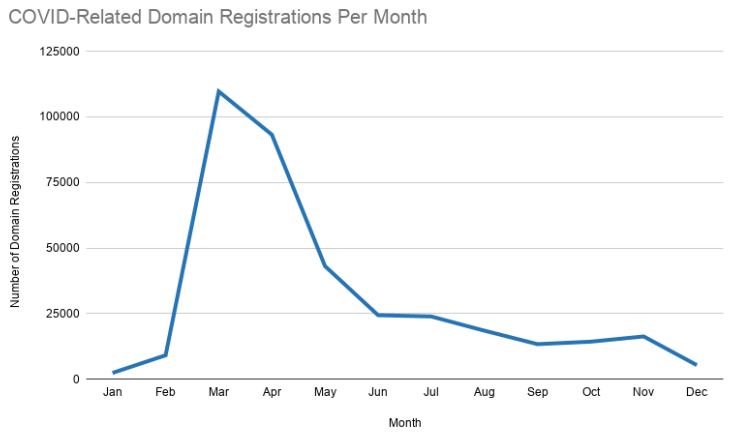


Figure 3: Total COVID-related domains registered per month from January 2020 through December 2020 (Source: Recorded Future)

According to Recorded Future data,the majority of domains related to COVID-19 were registered in March 2020 as seen in Figure 3, and monthly registrations continued to drop over the course of 2020. Public uncertainty about the virus and the desire for information were at a high in March, while the population was still working to establish its own understanding of credible sources of information and resources. It is important to note that not all of the registered domains were malicious, and the majority of the registrations appear to be opportunistic in nature.

Insikt Group defined a set of terms around five major themes and looked for the use of these terms in the newly registered domains since January 2020: "vaccine", "cleaning/ decontamination", "personal protective equipment (PPE)", "cures", and "economic relief". As seen in Figure 4 below, the domain registration curves for each thematic area closely follow the curve of overall domain registrations, as expected. Insikt Group observed a few interesting trends in the thematic data:

- Distinct spikes in testing- and vaccine-related domains occurred later in 2020. The first spike, around August, occurred around the time that Moderna and AstraZeneca were beginning their phase 3 trials of their vaccine candidates. Similarly, on August 12th, the Institute of Biology at the Academy of Military Medical Sciences approved the Sputnik V vaccine created by Gamaleya National Research Centre for Epidemiology and Microbiology. The spike in the registrations of vaccine-related domains starting in November correlates with the timelines of the conclusion of the Pfizer vaccine clinical trials, the subsequent release of the data to the FDA for approval (November 13, 2020), and the commencement of phase 3 trials for several vaccines around the world. The Pfizer vaccine, the first FDA-approved vaccine available for COVID-19, was approved by the FDA on December 11, 2020 and distribution to the population began. The registration of vaccine-related domains continued to climb sharply through December 2020; while some governments have begun creating legitimate websites to disseminate information about the vaccine, the same trend is visible, although to a lesser degree, in the domains that Recorded Future was able to classify as malicious (Figure 5, below). This suggests that while many domains were registered at these key stages in the development and approval of the vaccine, to date only a small subset have been identified as malicious, with a large majority not yet classified.
- Of the maliciously verdicted domains, two initial spikes in those related to "testing" occurred early in the pandemic. The first spike in testing-related domains occurred around the same time that tests in the U.S. were difficult to access (March and April), and that testing scams abounded. A timeline of COVID-19 tests per day can be seen in Figure 6, below, showing an increase over time.
- A spike in both overall domain registrations and maliciously verdicted domains related to "economic" terms, such as those themed around financial relief topics, occurred in August when the U.S. Congress increased discussions of a second COVID-19 stimulus bill. An additional spike in economic-related domain registrations beginning in October and going into November aligns with a large increase in mentions of unemployment fraud in the criminal underground during Q4 of 2020, as identified by Recorded Future.
- Domains related to non-vaccine and non-testing aspects of the pandemic such as PPE, cleaning and disinfection, and cures have experienced an overall decrease after the original registration spike starting in March 2020.

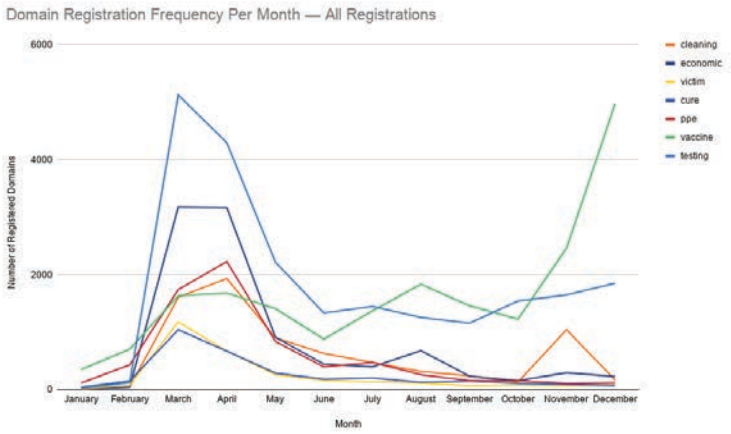


Figure 4: Themes identified in all COVID-19-related domain registrations and certificate registrations from January 2020 through December 2020 (Source: Recorded Future)

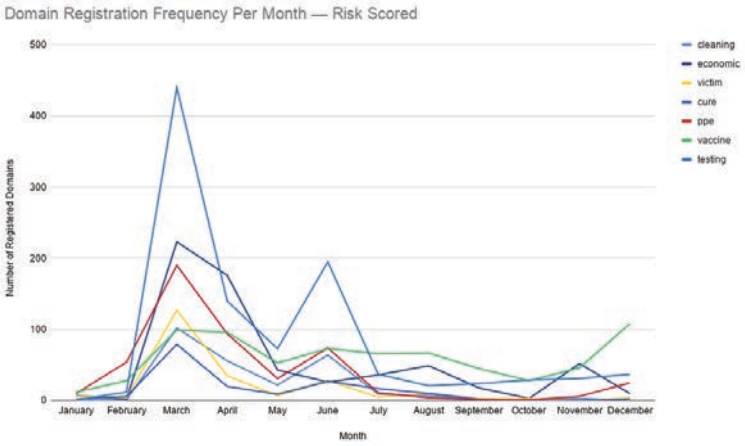


Figure 5: Themes identified in maliciously verdicted COVID-19-related domain registrations and certificate registrations from January 2020 through December 2020 (Source: Recorded Future)

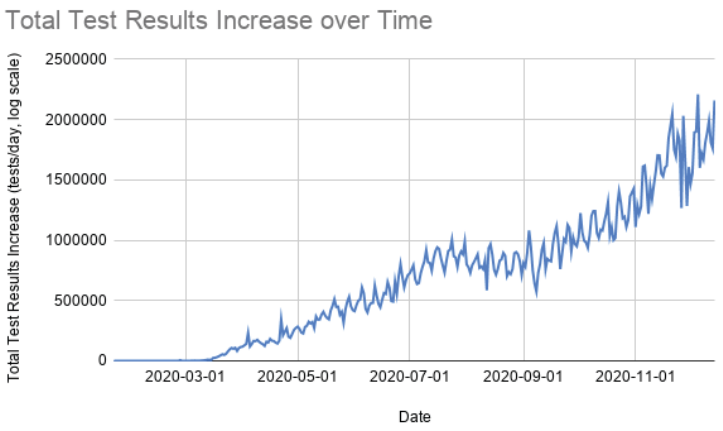


Figure 6: Total COVID-19 test results increase per day in the United States (Source: Covid Tracking Project)

The Economy of COVID-19

Insikt Group determined a few of the key markets and market sectors associated with the COVID-19 pandemic, including newly emerging markets, those that have experienced growth, and those that have been negatively impacted. While this list is not complete, Recorded Future used these as examples of the COVID-19 economy — industries and markets whose economic outcomes have been heavily influenced by the pandemic, particularly in areas that present opportunities for exploitation by threat actors.

Entities in the Healthcare Ecosystem

At the forefront of the pandemic economy has been the healthcare system and its supply chains — ensuring an adequate supply of medical resources ,access to care ,and medical personnel have been prolific talking points worldwide .Insikt Group has derived the following model of the main components of the healthcare ecosystem ,as seen in Figure ,7 below.

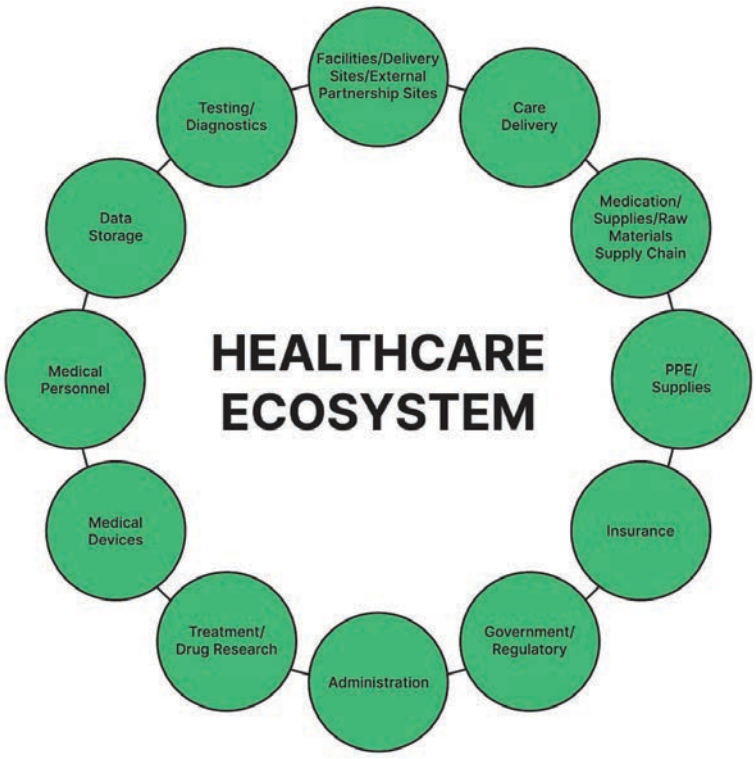


Figure 7: Entities within healthcare ecosystem (Source: Recorded Future)

COVID-19 diagnostics market: Expected to reach over $17 billion USD in the U.S. by the end of 2020. Includes PCR kits, point-of-contact kits, and immunoassays.

Global PPE market: The global healthcare PPE market is expected to grow from $5.99 billion in 2019 to $7.83 billion in 2020, with this growth primarily attributed to the COVID-19 pandemic.

Medical device market: The global medical device market was projected to be valued at $472 billion prior to the onset of the COVID-19 pandemic, but is expected to be valued at $461 billion, primarily as a result of declines and delays in elective procedures, and supply chain disruptions in raw materials and components, among other factors.

Hospital revenue: In the U.S., industry revenue for hospitals is projected to be $1,127.75 billion in 2020, a decrease from 2019 when it reached $1,188.91 billion. This decrease is primarily due to the decrease in elective surgery procedures and reductions in patients seeking preventative care.

Entities in the Vaccine Ecosystem

Recently, as the approval of a COVID-19 vaccine approached reality, additional focus on the "vaccine ecosystem" has emerged, especially the supply chain required to produce, store and distribute the vaccine. Insikt Group has derived a model of the main components of the "vaccine ecosystem" as seen in Figure 8, below.

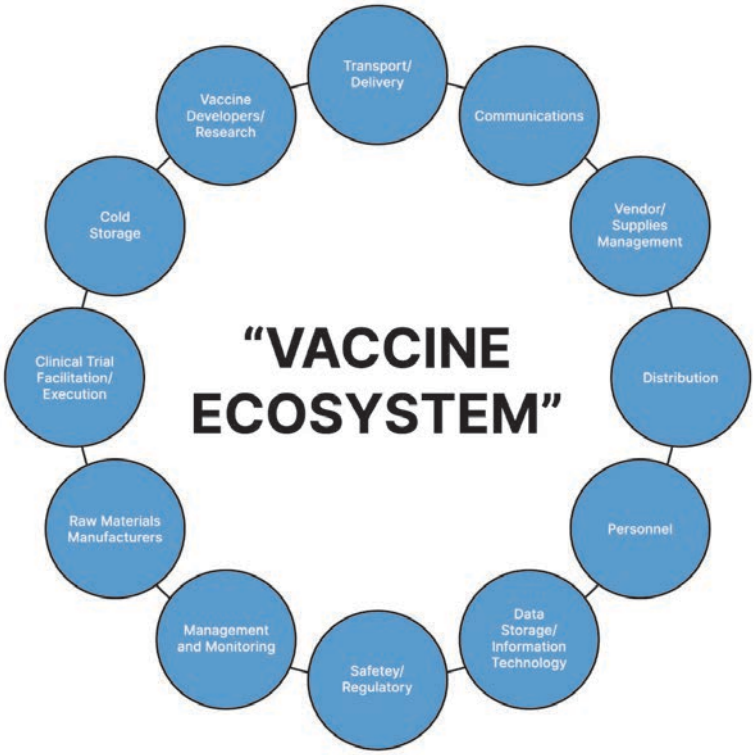


Figure 8: Entities within the vaccine ecosystem (Source: Recorded Future)

COVID-19 vaccine market: According to analysts at Morgan Stanley and Credit Suisse, the future value of the COVID-19 vaccine market could reach $10 billion USD across developed countries.

Cold chain market: The global cold chain market, which includes refrigerated transport and refrigerated warehousing, is expected to be valued at $233.8 billion USD in 2020. COVID-19 has impacted the industry through increased consumer demand for food products with longer shelf life, in addition to the need to transport and store at least one vaccine candidate at very cold temperatures. Companies that make up the cold chain, such as "freezer farms" and those that supply the components to them, are also in high demand.

Clinical trials market: The global clinical trials market is expected to grow at a compound annual growth rate of 5.1% from 2020 through 2027, up from $46.8 billion USD in 2019. Market drivers this year include the rapid development of COVID-19-related therapies and vaccines that require clinical trials and the fast-tracking of those trials, among other factors.

Market growth for the cold chain industry and in clinical trials further underscores the size of the "ecosystem" behind developing and delivering a successful vaccine, in addition to the size of the market for a COVID-19 vaccine itself. While it remains to be seen what role the delivery of the vaccine will play in the financial outlook of the freight and logistics market overall, this is yet another key component of vaccine delivery.

General Economic Entities Affected by COVID-19

Outside of healthcare, several industries experienced economic declines, due to the implementation of travel restrictions, border closures, and international attempts to stimulate the economy.

Tourism and Travel: The U.S. economy is predicted to lose $155 billion in 2020 due to the lack of international visitors and the virtual cessation of travel and tourism. In 2019, the market was valued at $145.27 billion, and in 2020, the market is expected to be valued at just $65.25 billion.

Energy Sector: An IEA study estimates a decline in global energy demand of 5% and corresponding waning oil and gas demands of 9% and 4%, respectively, by the end of 2020. With surplus supplies, the energy market is presently at a historic low.

Freight and Logistics market: The global freight and logistics market is expected to be valued at $835.06 billion in 2020. The impacts on different segments of the market varied; as a result of the pandemic, the industry saw increases in trucking volume of about 30% and 1000% surges in last-mile delivery, but also decreases in railroad volume of about 20%, and in ocean shipping of about 25%. Ultimately, the industry was negatively impacted by supply chain disruptions, limitations on transportation and international border closures, even as the share prices of delivery firms United Parcel Service (UPS) and Federal Express (FedEx) have risen.

Exploitation of Organizations Involved in the "COVID-19 Economy"

The primary goals of threat actors targeting organizations involved in the COVID-19 economy are disabling the organization's ability to perform a key function or stealing valuable data. While attacks on healthcare have received a lot of attention, the shift to remote work and the change in how services are delivered and consumed have affected a diverse set of organizations, including a 400% increase in attempted cyberattacks on the maritime industry, use of FedEx and UPS in phishing lures, and a data breach of the Small Business Administration (SBA) as businesses were applying for emergency loans.

The Healthcare Ecosystem

Markets within healthcare that presented strong opportunities for threat actors to exploit for financial reasons, primarily through scams and fraud, included COVID diagnostics and PPE, especially when the supply of both were low. Threat actors also exploited the strained healthcare system that experienced not only an influx of patients, but as previously noted, a decline in revenue due in part to the cancellation of elective surgeries. Insikt Group selected a subset of the components of the healthcare ecosystem to highlight the breadth of cyber events that have occurred:

PPE/Supplies:

- In late March 2020, a phishing campaign targeted a German multinational corporation that was associated with a task force to procure personal protective equipment (PPE), using fake Microsoft login pages to perform credential harvesting. While the attack was not attributed to a particular threat actor, the report from IBM notes that the initial malicious activity originated from a Russia-based IP address.
- Criminal threat groups have additionally exploited the disrupted PPE supply chain through non-delivery scams, the use of BEC against municipalities purchasing PPE or supplies, using a phishing lure pretending to be a business offering various types of PPE to deliver malware or selling counterfeit PPE and supplies.

Care Delivery:

- In 2020, there were several instances of threat actors targeting hospitals directly, particularly with ransomware. Most recently, attacks included Ryuk ransomware used against Universal Health Services in the U.S. (September 2020) and against several other hospitals in the U.S. (October 2020), and an unknown ransomware variant targeting Uniklinikum in Germany (September 2020), though attacks on hospitals that are suspected to be incentivized by the COVID-19 pandemic date back to at least early spring with the ransomware attack on Brno University Hospital (March 2020).

Treatment/Drug Research:

- Iranian hackers attempted to harvest credentials, including passwords, from Gilead Sciences employees in April 2020. Gilead is the maker of Remdesivir and at the time had been completing large-scale trials of the drug to evaluate its potential for treating COVID-19 patients.

Government/Regulatory:

- In January 2020, APT32, a threat actor group suspected to be Vietnamese, carried out phishing campaigns against Chinese targets including China's Ministry of Emergency Management and the government of Wuhan province with the goal of acquiring more information about the emerging pandemic.
- The U.S. Health and Human Services Department (HHS) suffered a cyberattack by a suspected foreign actor in March 2020. The goal of the attack was suspected to be to undermine the agency's COVID-19 pandemic response.

While this list of cyber incidents is not complete, it suggests that threat actors continue to target overburdened healthcare organizations due to the likelihood that these organizations' are focusing resources towards patient care, and possibly away from cybersecurity. Attacks on U.S. hospitals continued throughout the year, as seen in Figure 9 below, though two spikes occurred in the activity — a smaller one in May, and a larger one in September. These spikes align, though weakly, with the U.S. hospitalization trends seen in Figure 10. Fraud and scams related to PPE primarily occurred earlier on in the pandemic, during March and April, when there were widely publicized shortages.

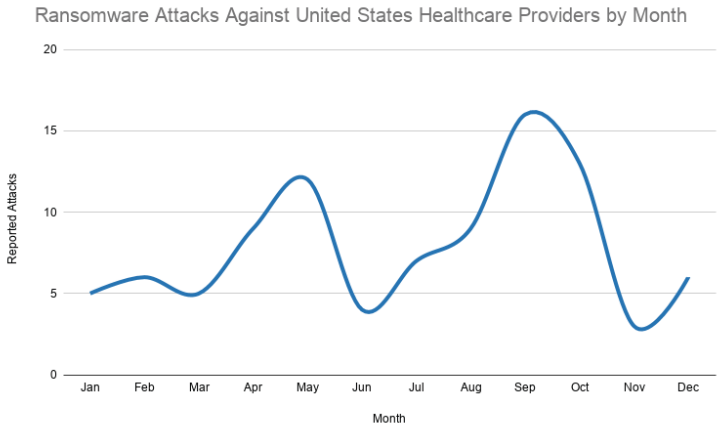


Figure 9: Number of reported ransomware attacks against U.S. healthcare providers by month in 2020 (Source: Recorded Future)

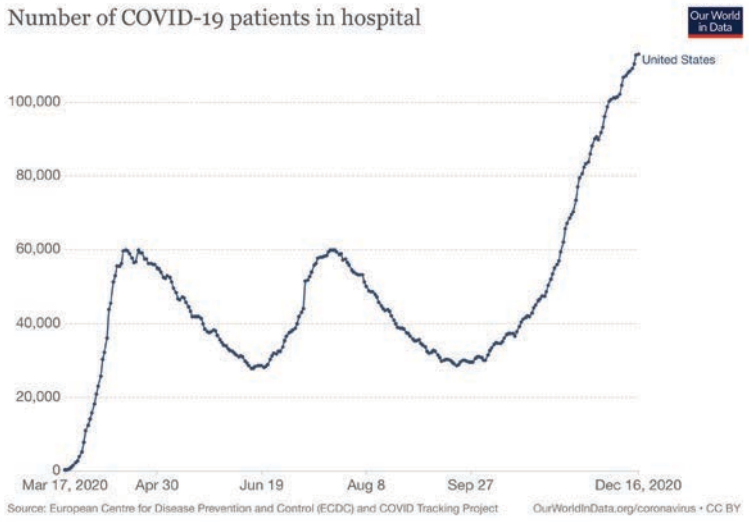


Figure 10: Current number of COVID-19 patients in the hospital in the U.S. (Source: OurWorldInData.org)

The Vaccine Ecosystem

Four nations are suspected to have directly targeted organizations involved in the development, delivery, or production of the COVID-19 vaccine: Russia, China, Iran, and North Korea. Insikt Group selected a subset of the components of the vaccine ecosystem to highlight the breadth of cyber events that have occurred.

The pandemic has negatively impacted many countries economically, and for many of those, a successful vaccine was seen as the only way back to a thriving economy, suggesting a major incentive for attacks on vaccine research and development. Later, once late-stage clinical trials began to conclude worldwide, and approvals of the vaccine candidates appeared likely in Western countries (such as the U.S. and U.K.), threat actors changed the focus of some of their attacks to target the supply chains behind the vaccine in order to complicate

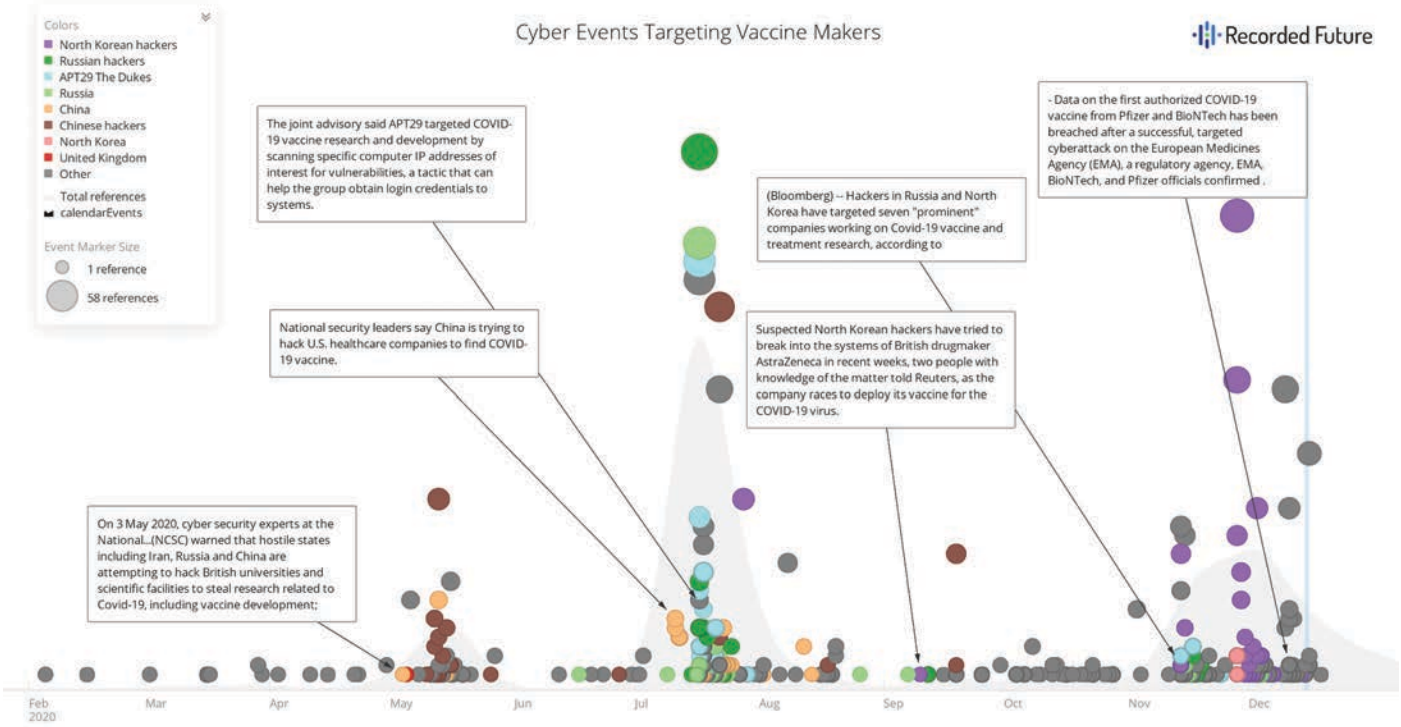


Figure 11: Cyber events targeting vaccine makers throughout 2020 (Source: Recorded Future)

distribution, delivery, and storage. These attacks were not only limited to the companies strictly involved in the vaccine, but non-governmental organizations (NGO) and government entities engaged in the facilitation of the distribution process. Finally, the launch of Russia's vaccine disinformation campaign sought to damage the industry's communications around the safety and efficacy of at least one vaccine candidate.

Vaccine Developers/Research:

Information theft from organizations involved in vaccine research and development was a common motivator, both prior to the development of a vaccine known to work against COVID-19 and, to some degree, after various candidates were approved around the world. Some of the particularly notable incidents are as follows:

- APT29 (also known as "The Dukes"), a Russian state-sponsored threat activity group, targeted several organizations involved in the development of the COVID-19 vaccine in July 2020 using malware called WellMess and WellMail. The primary motivation of the attacks is thought to be intelligence-gathering.
- APT28, also known as Strontium or FancyBear, is a Russian state-sponsored threat activity group who targeted pharmaceutical companies and organizations developing vaccines in several countries using password spray and brute force login attempts.
- Russia launched a disinformation campaign in October 2020 to manipulate the public into buying the still-untested Russian vaccine, Sputnik V. The campaign spread false information wrongfully claiming that Oxford University's COVID-19 vaccine used monkey DNA as a vector for development, saying that it would turn humans into monkeys.
- Suspected North Korean groups Zinc (also known as Lazarus Group) and Cerium (linked to Kimsuky based on infrastructure overlaps), targeted pharmaceutical companies and organizations developing vaccines in several countries using spearphishing for credential theft. It is suspected that North Korean threat actors have attempted to break into at least nine health organizations, including vaccine makers such as AstraZeneca, Johnson & Johnson, and Novavax Inc.
- In July 2020,the U.S. Department of Justice proclaimed in an indictment that Chinese state-sponsored threat actors attempted to probe the networks of vaccine research organizations. News outlets later revealed that one of the targets was Moderna Inc., a vaccine developer.

- A network intrusion targeting the European Medicines Agency (EMA) in December 2020 resulted in the theft of documents related to the development of vaccine candidates by Moderna Inc and Pfizer Inc./BioNTech that were submitted for the approval process. The attack is unattributed as of this writing.
- Though specific incidents were not specified, Chris Krebs, former CISA Director, noted that Iran was among the countries whose state-sponsored attackers "doing some kind of espionage or spying, trying to get intellectual property related to the vaccine".

Cold Storage:

- Americold, a cold storage company that was in talks with vaccine manufacturers to provide cold storage and transport to enable vaccine delivery, was hit by a suspected ransomware attack in late November 2020. As of this writing, the attack remains unattributed.
- In December 2020, IBM reported on a phishing campaign dating back to September 2020 that spanned across six countries, targeting organizations associated with Gavi, The Vaccine Alliance's Cold Chain Equipment Optimization Platform (CCEOP) program. While the attack is unattributed as of this writing, the purpose appears to be the collection of credentials to enable future unauthorized access to the organizations.

Data Storage and Information Technology:

- IBM also reported that South Korean and German firms providing software and web development services for organizations in the transport, pharmaceutical, and manufacturing industries, among others, were victims of the COVID-19-related phishing attempts.

Safety and Regulatory:

- IBM identified the European Commission's Directorate-General for Taxation and Customs Union as another target of these phishing attacks, noting that the organization "could serve as a single point of compromise impacting multiple high-value targets across the 27 member states of the European Union and beyond"

Clinical Trial Facilitation and Execution:

- A ransomware attack on eResearchTechnology, a company that sells software used by several clinical trial providers, disrupted aspects of clinical trials at IQVIA (AstraZeneca's COVID vaccine trial) and Bristol Myers Squibb (part of a consortium developing a quick test for the virus).
- Dr. Reddy's Laboratories, a pharmaceutical company based in India, experienced a ransomware attack on its servers days after receiving approval to conduct clinical trials of a COVID-19 vaccine candidate.
- In March 2020, a contract research organization (CRO) based in London working on COVID-19 projects with the U.K. government experienced a Maze ransomware attack. While the CRO was able to stop the attack prior to file encryption, the threat actors were able to steal data, including patient information, that they used to attempt to extort payment

Distribution:

- Once the U.K. began distributing the approved vaccine, criminal threat actors began scams advertising "tested" COVID-19 vaccines for sale. Fake vaccines have been advertised on the dark web since April, but after the approvals of the vaccines in the U.S., online scams around gaining access to these vaccines have increased. Recorded Future has no evidence that these vaccines are legitimate or have been diverted from intended recipients.
- COVID-19 vaccine scams have also been employed to gather victims' PII or financial information and for financial gain through offerings such as early access to the vaccine for a price and access to clinical trials.
- APT28 used a phishing lure about "Sinopharm International Corporation" to deliver the Go version of the Zebrocy malware.

The General Economy

Outside of the healthcare and vaccine industries, general economic suffering resulting from secondary effects of the COVID-19 pandemic presented additional areas of opportunity for threat actors to adapt their TTPs to target victims as the public's concerns around the pandemic evolved.

- As the financial impacts of business shutdowns and furloughs continue, financial relief has emerged as a lucrative target, especially as it relates to small businesses and unemployed individuals. Scams involving donations to fake charities, sites fraudulently purporting to offer small business loans or impersonating the Small Business Association (SBA) have occurred throughout the pandemic. Unemployment during the pandemic has reached a record high, and cybercriminals have executed numerous scams. These include using spoofed websites to harvest PII to conduct fake hiring scams, fraud targeted at state unemployment insurance programs, and Pandemic Unemployment Assistance (PUA) claims.

- Scams have targeted the tourism travel industry, focused on fake offers of travel insurance that included cancellation due to COVID-19-related reasons. However, Insikt Group did not observe any large-scale cyberattacks targeting the travel and tourism industry, most likely due to the large overall decrease in the industry worldwide.
- Nearly a year into the pandemic, it is clear that COVID-19 restrictions have affected cartel activity across not only Latin America, but globally. New restrictions have led to increased competition for local markets and have forced cartels to adapt their business models, already resulting in changing patterns of violence as cartels seek to improve their standing and develop new revenue streams. With most nations hardening borders, the illegal drug market has faced long-term disruptions, pushing organized crime groups to find alternative channels for supply and distribution. Furthermore, Mexican cartels have used the pandemic as a means to garner support from locals by distributing care packages in hopes that it will be sufficient to place them in local elections where pro-cartel policy can be enacted and have enforced regulations that typically fall under the purview of government authorities, such as imposing curfews and providing material aid.
- Compared with 2019, cyberattacks on the shipping industry increased in 2020. The shipping and logistics industry was primarily impacted by the COVID-19 pandemic through the increased number of employees working from home, supply chain disruptions and increased demand in some of its sectors (especially trucking and "last mile" delivery). Over the course of the year, attacks against logistics companies included ransomware (such as Maze targeting Pitney Bowes, Nefilim targeting Toll Group and a Ragnar Locker attack on CMA CGM), and phishing lures using logistics company brands (including DHL, Maersk, UPS and FedEx). While it is not possible to say how substantial a factor the pandemic was in these attacks, the use of shipping companies in phishing lures as "trusted brands" was often in association with COVID-19 during the beginning of the year.
- With the move to working from home, energy demands increased in residential locations and decreased in commercial and industrial spaces and transportation (particularly in aviation and public transport). To date, there has not been a "massive flood" of attacks, despite the increased cyber risk in the industry due to the increase in remote work and changing energy demands
- Early on in the pandemic, as employers started asking employees to work from home, Recorded Future noted an increase in the attack surface companies now faced due to the sudden change in network topology and increased use of remote work applications.

Targeting Through Disinformation

From the onset of this pandemic, information has been used as a tool for both the benefit and the detriment of global citizens. Governments, politicians, corporations, and criminals have abused technological resources such as social media, media outlets, and television to confuse the public by spreading disinformation to control the narrative for financial, political, and ideological gain. In times of global uncertainty, information is used in a battle for power and influence through disinformation and influence operations.

China made significant efforts to control the narrative about its handling of COVID-19 in an effort to save face and present itself as a strong and capable world power. Meanwhile, their troll farms and state-affiliated media criticized the U.S. and U.K. as COVID-19 statistics climbed in those countries, reinforcing their views that the Chinese system of governance was more successful than others. China continues to aggressively pursue global economic growth and their long-term objectives, and maintaining a good reputation is one of their primary strategies.

Russia's disinformation arm has also focused on discrediting Western democratic government policies around COVID-19, and amplifying positive sentiment around their own handling of the pandemic in an effort to glorify the Russian system of rule and draw international respect. Russia used state-affiliated media, social media, diplomats, and political leaders, as well as proxy and fake news sites, to push these narratives and spread false information within Western countries. One of the most dangerous disinformation tactics Russia uses is infiltrating adversary social media to instigate civil conflict and incite violence during times of crisis. This tactic was used widely throughout the 2020 COVID-19 pandemic in the United States and the U.K.

Insikt Group Observations of COVID-19 Information Manipulation In 2020

At the beginning of the pandemic, rumors about how COVID-19 spreads, its symptoms, and its fatality rate were widespread. Every media channel and millions of people on social media speculated and shared unconfirmed stories about the disease, creating confusion and conflict, and undermining medical authorities such as the World Health Organization (WHO) and the U.S. Center for Disease Control (CDC). Scientists who had valuable data to share with the world were silenced in favor of political spin and corporate profit.

A study of COVID-19 messaging on social media revealed misinformation from politicians, celebrities, and other prominent figures made up about 20% of claims but accounted for 69% of total social media engagement. This level of misinformation results in the serious risks to human lives throughout the world. According to another study published by the private-sector National Bureau of Economic Research, U.S. audiences that were exposed to television programming that downplayed the severity of the pandemic saw greater numbers of cases and deaths — because people didn't follow public health precautions.

The Origin Blame Game

From the outbreak of the 2019 novel coronavirus in China, governments around the world were quick to blame China for the virus. It was not long before unsubstantiated rumors began to spread that it was a man-made biological weapon, and China was quick to defend itself and save face on the global stage. Public criticism of China's handling of the viral outbreak from U.S. politicians and leaders led to a significant increase in unfavorable views of China by mid-2020. A Pew Research study reported that by July 2020, 78% of Americans blamed the Chinese government for the global spread of the coronavirus. Recorded Future found that China quickly countered this narrative using state-sponsored media to emphasize two points: First, that China was being transparent and helpful to the international community, and second, that the spread of the virus to new areas was limited. In March, China began pushing a new theory that the novel coronavirus is an American disease that was introduced by members of the U.S. Army who visited Wuhan in October for the Military World Games. In November 2020, China again shifted blame for the origin of COVID-19, this time to India.

Despite efforts to shift blame, COVID-19 began spreading across China. One Chinese ophthalmologist, Dr. Li Wenliang, began speaking out publicly about the virus, warning the world of how deadly and fast-spreading the virus really was. In an attempt to suppress this information, the Chinese government began censoring Dr. Li's statements from state-affiliated media and social media outlets. However, when Dr. Li Wenliang died from COVID-19 on February 7, 2020, Chinese citizens were enraged at the government's handling of the situation, as they grieved the loss of a doctor who strived to warn the world of the gravity of COVID-19.

In late January, Russian officials began spreading theories that COVID-19 is an American biological weapon or a plot for pharmaceutical companies to enrich themselves. The rumors became more descriptive as Russian state-affiliated media and politicians continued to propagate the narrative that the U.S. created COVID-19 as a weapon to cripple Chinese economic growth. Russian disinformation is not a new tactic of manipulation, and the methods they use are generally consistent across decades. The false information usually starts in fringe media outlets and then is shared and amplified by state-affiliated media outlets, Russian diplomats, and notable figures. Although the majority of the COVID-19 disinformation was amplified in the Russian language, there were many instances where they were translated into English for a broader audience.

In May 2020, a YouTube video emerged of discredited scientist Dr. Judy Mikovits defending a conspiracy theory that COVID-19 was designed by the global elite to gain power and money, accusing Dr. Anthony Fauci, Bill Gates, and others of being involved in the conspiracy. The video, a shorter clip from the film "Plandemic", was picked up by various conspiracy theory groups such as anti-vaccinators, QAnon, and fringe media outlets such as Epoch Times and Gnews[.]com. The video garnered over 8 million views and Dr. Mikovits' name accrued millions of hashtags and mentions across various social media platforms. This example defines the challenges of controlling unverified scientific theories and medical disinformation in the age of COVID-19.

COVID-19 Safety and Protection Rumors

Disinformation around COVID-19 safety and protection created a ripe environment for scammers and fraudsters to take advantage of a largely ignorant public. The public did not know what to believe or who to listen to, which led to additional conspiracy theories. When authorities began making recommendations for wearing personal protective equipment (PPE) to protect from COVID-19, misinformation about the efficacy and availability of PPE began spreading rampantly. Hospitals and healthcare facilities were running short, and imports of masks, gloves, and gowns were in low supply. Rumors were muddled among scientific and medical explanations on topics such as how long the virus lives on surfaces, the efficacy of different types of masks, how it spreads from person to person, and what temperatures the virus can survive in. The confusion led to panic. Retailers and scammers alike began to mark up prices on handmade masks and alcohol-based sanitizer products. Hospitals were reporting shortages of PPE, and President Trump denied those claims, calling it "fake news".

Mitigations

As the pandemic evolves, threat actors will continue exploiting the most "lucrative" opportunities for access to traditional and new targets. Recorded Future recommends that organizations continue to educate employees about new tactics that threat actors are using, including phishing lures, scams, and fraud exploiting the pandemic. Additionally, awareness of disinformation and sources of credible information is key to helping individuals avoid manipulation and foreign interference as the pandemic progresses. Additionally, we recommend the following steps to combat COVID-19 disinformation:

- Share data sourced from science and trusted public health officials. Public health officials should seek out social media influencers to amplify truthful fact and science-based information about COVID-19.
- Public health officials and social media companies have to work together to flag and take down misinformation around COVID-19. 39% of misleading statements in social media are related to the actions and policies of public authorities. Confirming and denying statements can help security teams flag false information.
- Detect, understand and expose COVID-19-related misinformation through data science and behavioral analytics.
- More advice on how to tell facts from misinformation can be found here.

Outlook

While both state-sponsored and criminal threat actors have employed the COVID-19 pandemic to further financial, espionage, and intelligence-gathering goals, it is apparent that the way in which they do so is largely related to the larger socioeconomic situation. As the pandemic itself continues to evolve, and with the introduction of approved vaccine candidates in several countries, distribution of these vaccines, and the beginning of economic recovery, Recorded Future expects to see the focus of cyberattacks shift again. Future attacks will likely seek to negatively impact each of these areas, particularly:

- Criminal threat actors will likely continue to target industries and organizations focused on the delivery of the vaccine, especially as distribution increases and these organizations become increasingly appealing targets. This will most likely be through attempting to disable the organizations, such as through ransomware attacks.
- Both criminal and state-sponsored threat actors may target PII or patient data of those who have been vaccinated or have participated in vaccine trials, or test results of these individuals.
- State-sponsored threat actors will continue to conduct malicious disinformation campaigns to target adversaries and global society in an effort to gain economic and political advantage.
- Threat actors may seek to discredit the vaccines as "dangerous" or "ineffective" and continue the narrative that vaccines are being used to "track" individuals to further sow distrust.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.