BlueVoyant®

2020 NOVEMBER BIOTECH AND PHARMACEUTICAL REPORT

CONTENTS

Analysis revealed that attacks on biotech and pharmaceutical organizations are on the rise - leaping by

50%

from 2019 to 2020

EXECUTIVE SUMMARY

The global COVID-19 pandemic has put a spotlight on the world's biotech and pharmaceutical industries. News about potential vaccines has driven surges in company stock prices;

optimism in vaccine development may be responsible for buoying the stock market in its entirety[1]. This has also resulted in some of the highest-profile nation-state cyberattacks in recent memory. Between May 2020 and August 2020, United States federal agencies accused both Russian and Chinese cyber espionage groups of attempting to steal COVID-19 vaccine information from developers.[2][3] In a world facing a global pandemic, no industry is under greater scrutiny or plays a more critical role than the pharmaceutical sector.

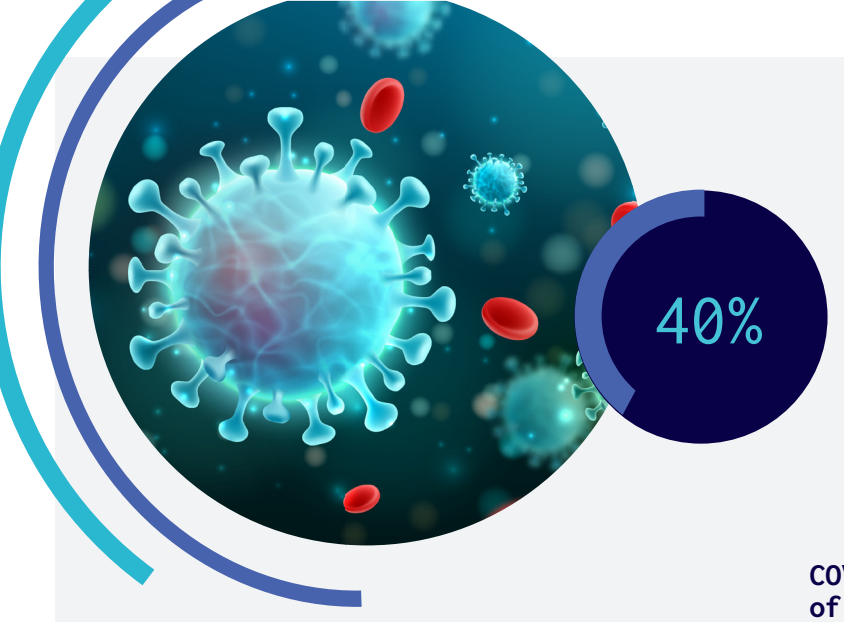
Attacks on pharmaceutical companies are not new. As a key part of the global healthcare sector, pharmaceutical and biotech companies are targeted by the same sophisticated nation-state groups that seek to disrupt critical industry for geopolitical advantage. However, these companies also deal in some of the world's most critical and priceless intellectual property (IP), and as a result operate at risk from opportunistic and highly capable cybercriminals who seek to steal and exploit their data.

In this report, BlueVoyant examines the biotech and pharmaceutical industries during the most critical time in their existence. Analysis reveals an industry under aggressive and targeted attack; unfortunately, it also reveals an industry often lacking critical protections needed to defend against the threats it faces.

Analysis revealed that attacks on biotech and pharmaceutical are on the rise - leaping by 200% from 2017 to 2018, jumping again by 50% from 2019 to 2020. Despite almost half of all attacks being due to ransomware, the industry too frequently lacked critical defenses against phishing and remote desktop exploits: methods most favored by ransomware groups. And attackers worldwide have responded actively to the race for a COVID-19 vaccine - by massively ramping up attacks on companies developing vaccines.

COVID-19 has changed the scale and specificity of attacks - meaning companies with access to key technologies struggle to defend themselves, now when they are most necessary. As always, inspired and directed by the core mission of collective defense, BlueVoyant seeks to support and empower those in the biotech and pharmaceutical industries to defend themselves at a critical juncture for the industry and for healthcare everywhere.

[1] https://www.marketwatch.com/story/are-stock-market-investors-overpricing-or-underpricing-a-potential-coronavirus-vaccine-2020-08-22
[2] https://www.washingtonpost.com/national-security/us-china-COVID-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0_story.html
[3] https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF



Of 25 attacks reported in the media since 2017, ten - or 40% - occurred in 2020 alone

KEY FINDINGS

Attacks on biotech and pharma companies are on the rise

Analysis of open-source reporting on attacks on biotech and pharmaceutical companies since 2017 showed that attacks on biotech and pharmaceutical companies are on the rise. Of 25 attacks reported in the media since 2017, ten - or 40% - occurred in 2020 alone. The rise in attacks was driven by the accelerating rate of ransomware incidents, beginning in 2018. It was also augmented by the race for the COVID-19 vaccine, which resulted in several publicly disclosed attacks on U.S. pharmaceutical firms by nation-state actors. No doubt there are more that are unreported (and many more that are undetected).

Many biotech and pharmaceutical companies are vulnerable to ransomware

While the number-one threat driving the 2020 headlines is nation-state espionage looking to steal COVID-19 vaccine research, the top threat for most biotech and pharmaceutical companies is still ransomware, making up almost half of all reported attacks. Critically, a number of pharmaceutical and biotech companies remain vulnerable to ransomware. Key defenses against targeted ransomware attacks, especially securing open remote desktop access ports and phishing security, were not seen implemented across most observed companies.

Analysis of threat intelligence data shows that biotech and pharmaceutical companies are under massive and daily attack

Using proprietary datasets and tools, BlueVoyant analysis revealed that the largest biotech and pharmaceutical companies in the world face massive and constant malicious inbound traffic. Most of this traffic is merely scanning, but much includes more targeted incidents: brute force attacks, phishing attempts, and identification and targeting of vulnerable web applications.

COVID-19 vaccines are the crown jewels of 2020 - and cyber attackers know it

All pharmaceutical and biotech companies that BlueVoyant observed had evidence of malicious targeting. However, the 8 most prominent companies in the race for the COVID-19 vaccine faced high volumes of targeted, malicious attacks - often out of proportion to their size, and much more than larger, more well-known pharmaceutical giants.

In addition, active malicious domains that sprung up in the wake of COVID-19 were seen focusing on pharmaceutical companies with targeted campaigns. In at least four companies, BlueVoyant data suggested that there was some evidence these campaigns may have succeeded.

The 8 most prominent companies in the race for the COVID-19 vaccine faced high volumes of targeted, malicious attacks

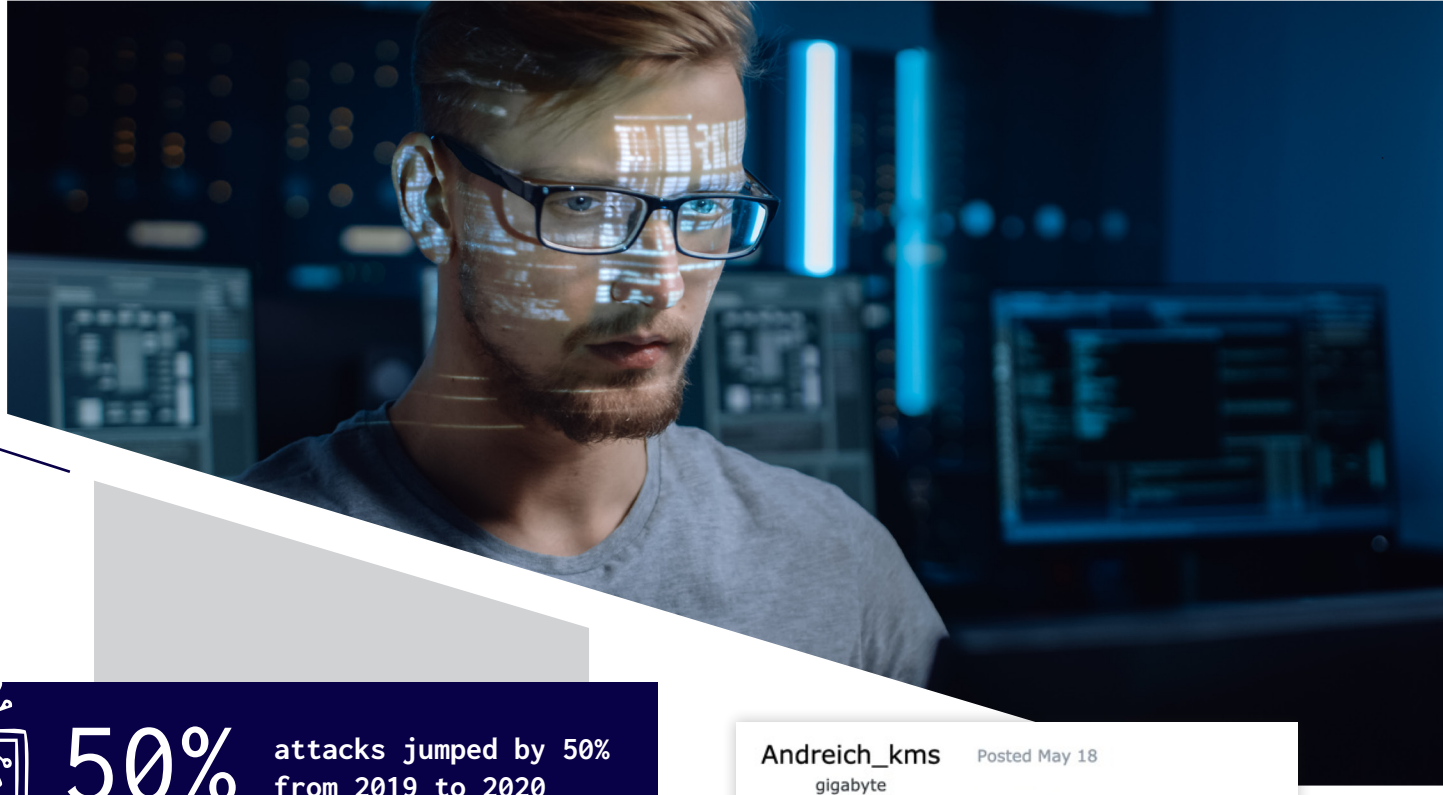
OVERVIEW AND TIMELINE OF MAJOR PHARMACEUTICAL CYBER ATTACKS

The first high-profile attacks against pharmaceutical companies came in 2017 - with the global WannaCry and NotPetya attacks. Along with many other partners in the healthcare industry and beyond, some large pharmaceutical businesses found their operations and networks ransomed by malware. However, these were not the first cyberattacks against the industry, and certainly not the last.

Healthcare, more generally, has long been a target of nation-state actors. As a critical industry, healthcare represents a useful lever for geopolitical advantage in competitions between states that continue below the threshold of armed conflict. As such, these large pharmaceutical businesses found themselves on the receiving end of ransomware strains developed by North Korea and Russia, shutting down systems as part of a wider and geopolitical contest.

However, pharmaceutical companies are also a major and consistent target for financially motivated cybercriminals. While the global search for a COVID-19 vaccine has elevated this to the level of international attention, pharmaceutical and biotech companies have been on the receiving end of cybercriminal attacks for several years. Pharmaceutical companies develop highly lucrative IP; they often handle large amounts of patient and other healthcare data; and as such, they exist as prime targets for criminals looking to compromise, steal, and exploit that information.

Pharmaceutical companies develop highly lucrative IP; they often handle large amounts of patient and other healthcare data; and as such, they exist as prime targets

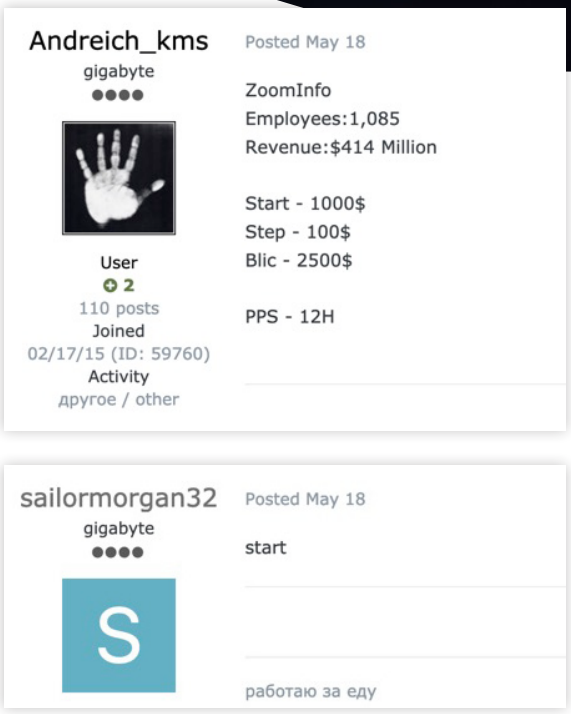


50% attacks jumped by 50% from 2019 to 2020

It is clear from an analysis of attacks publicly reported in open-source media that incidents involving biotech and pharmaceutical companies are on the rise.

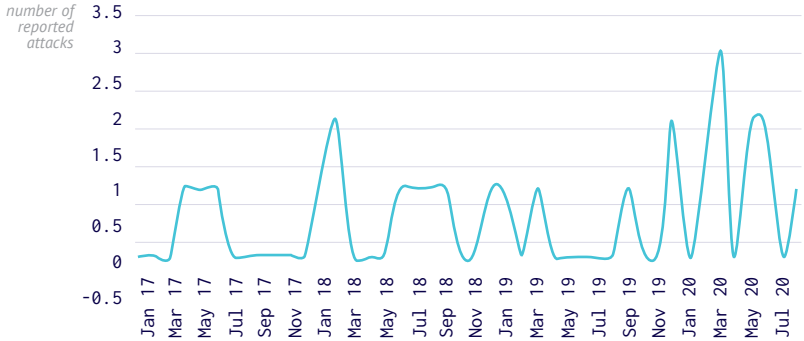
BlueVoyant analysis examined open-source records for all incidents related to biotech and pharmaceutical companies in the last four years, beginning in 2017. Attacks jumped by over 200% from 2017 to 2018, the year ransomware really took flight; and jumped 50% again from 2019 to 2020.

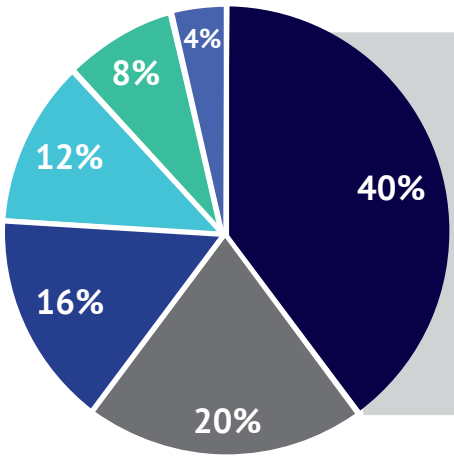
Moreover, while attacks varied - including spear phishing attacks that led to infostealers and other kinds of malware, data breaches, attacks and leaks by insiders, and unknown attacks (occasionally led by nation-state actors, as during the COVID-19 vaccine race) - the overwhelming preponderance of attacks were ransomware.



Screenshot of a cybercriminal offering access to a [redacted] pharmaceutical company on a dark web forum.

TIMELINE: JAN 2017 - JULY 2020





THREAT INTELLIGENCE RESEARCH

BlueVoyant analysts set out to identify key risks to biotech and pharmaceutical companies based on certain premises. The first, as determined by news reports of nation-state attempts to steal COVID-19 vaccine data, is that biotech and pharmaceutical companies were under threat. What does that mean? Are vaccine-developing companies under more threat? How has COVID-19 changed the threat landscape?

The second premise was determined by an analysis of open-source material, as outlined above. If ransomware is the number one threat vector for this industry, then what are the key risks for biotech/pharmaceutical companies, and what is necessary to mitigate those risks?

In order to investigate these issues deeply, BlueVoyant analysts chose **20 companies** on which to conduct passive, but in-depth, observation and analysis. These companies included 12 of the largest biotech and pharmaceutical companies in the world, as well as the eight companies that were most active in developing a COVID-19 vaccine as of July 2020.

The companies were as follows:

1. GlaxoSmithKline*
2. AstraZeneca
3. Pfizer*
4. Merck
5. Novartis
6. Roche
7. Johnson & Johnson*
8. Novo Nordisk*
9. Sanofi
10. Alexion
11. Regeneron
12. Vertex
13. Incyte
14. Biomarin
15. Jazz
16. United Therapeutics
17. NovaVax*
18. Moderna*
19. SinoVac*
20. CanSino*

Companies with an asterisk (*) were, at the time of writing, identified as leading in the development of the vaccine[4]. Since then, some others (notably Merck) have announced partnerships or their own late-stage entry into the vaccine race.

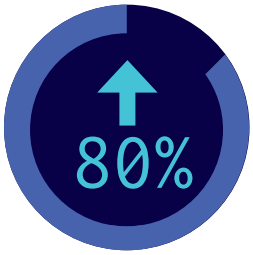
BlueVoyant analysis went further than open source review. Using proprietary datasets and tools, BlueVoyant examined these companies' preparedness against potential ransomware attacks; reviewed traffic data for any malicious targeting; and examined if any specific activities were targeting COVID-19 leaders. BlueVoyant analysis determined three key findings, as enumerated at the start of this report. Those were:

1. Using the selected biotech and pharmaceutical companies as a representative sample, it is evident that companies in this sector face high volumes of malicious inbound traffic on a daily basis. Furthermore, much of this traffic is highly targeted;

2. Despite several years of consistent ransomware attacks, a number of these biotech and pharmaceutical companies still do not use basic protections against the most common avenues of attack;

3. The highest volume of inbound targeting was observed in companies seeking a COVID-19 vaccine, not in the largest or most traditionally 'well-known' businesses - and COVID-19-related phishing and malware scams were targeting pharmaceutical companies across the board.

[4]https://www.biopharmadive.com/news/coronavirus-vaccine-pipeline-types/579122/



OVERALL THREAT LANDSCAPE

The breakdown of 20 companies found 80% show signs of more targeted activity

Almost every company with an online presence faces some form of traffic of ill intent. In 2020, a great deal of this traffic is driven by botnets[5] which have risen again in the last several months to make up a large proportion of the internet's unwanted traffic[6].

All of the 20 observed pharmaceutical/biotech companies had some form of malicious traffic directed towards their networks. These are not simply companies with an online presence - these are global, high-profile businesses, which means it is no surprise that they face high volumes of suspicious traffic directed their way: whether from automated bots and scanners or from opportunistic cyber actors.

BlueVoyant analysis digs deeper, however, to determine what degree of this traffic is more targeted and sophisticated. 'Targeted' activity means any inbound traffic that shows signs of more malicious, intentional, and focused efforts. Is the traffic anonymized, and probing at vulnerable webpages? Is the traffic focused on login webpages and showing signs of programmatic behavior, such as observed in brute force or credential replay attacks? When we strip away botnets and scanners, does the remaining traffic appear to be from malicious actors tied to specific malware families or known exploits?

The breakdown of 20 companies shows that all face some level of malicious inbound activity. More concerning, the majority - 80% - show signs of more targeted activity.

Even more troubling, over a quarter demonstrate some signs of compromise. Seven of 20 companies showed outbound traffic reaching out to known malicious domains and IPs - suggesting compromised devices or networks.

20/20

Observed evidence of malicious inbound traffic

16/20

Observed evidence of targeted malicious inbound traffic

7/20

Observed evidence of compromise

[5]https://www.bitdefender.com/box/blog/iot-news/iot-botnet-attacks-rise-2020/#:~:text=The%20first%20half%20of%202020,a%20report%20from%20Nozomi%20Networks.
[6]https://blog.checkpoint.com/2020/03/11/february-2020s-most-wanted-malware-increase-in-exploits-spreading-the-mirai-botnet-to-iot-devices/

Of those showing signs of targeted activity, the breakdown is as follows:

Targeted malicious traffic

16/20
Observed

4/20
None

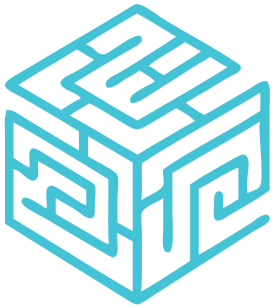
15/20
Brute force attacks

15/20
Target exploits and malware

6/20
Anonymized probing

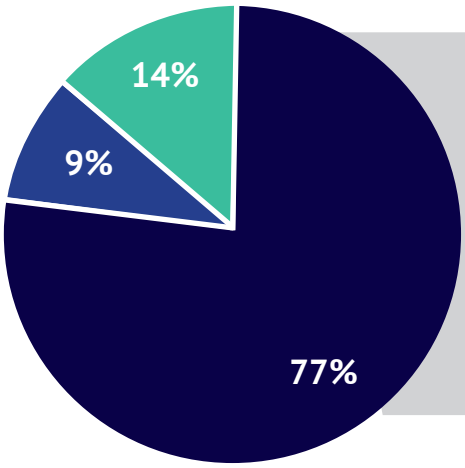
This has several implications. First, biotech and pharmaceutical companies face nearly universal (80%) targeted, intentional probing. Second, these attackers are using automated tools and infrastructure - three-quarters used programmatic brute force attacks, meaning they acquired a credential database and then built or bought an automated program (probably a bot) to target specific companies. Others still were more sophisticated: they were using command and control infrastructures bought and built for targeted exploits and malware. Another group was making use of anonymizing tools to hide their activity. These are serious and intentional actors.

The third and last implication is that these incidents occurred without regard to a company's size or area of focus or geography - while the volume of attacks followed some observable pattern (on which more below), the wide distribution of attacks did not follow a pattern. Which means that if you are a biotech company, you are likely to be under attack from sophisticated and knowledgeable cyber actors.



If you are a biotech company, you are likely to be under attack from **sophisticated** and knowledgable cyber actors

77% of companies had both unsecured RDP ports and email domains lacking basic security measures



RANSOMWARE VULNERABILITIES

A review of attacks over the last three years demonstrates that ransomware is the number-one threat to biotech and pharmaceutical companies - comprising almost half of all attacks. Moreover, the spectre of WannaCry and NotPetya three years ago still looms large in the memory of the cybersecurity and infosec community. So how have biotech and pharmaceutical companies responded to this threat?

Ransomware groups are many: recent BlueVoyant reports have analyzed activity by Ryuk, REvil/Sodinokibi, Netwalker, Nefilim, and of course Maze. While each group's code is different, these malware groups follow extremely similar techniques, tactics, and procedures (TTPs), which rely overwhelmingly on exploiting remote desktop vulnerabilities[7] and phishing[8]. While phishing is the eternal cyber threat, remote desktop protocol (RDP) vulnerabilities have become even more critical in 2020 as companies rely more heavily on employees working from home.

For companies, this means that defense relies on securing RDP ports (or at least limiting their access to authorized users) - ports critical for allowing remote work environments - and implementing security configurations to prevent phishing. BlueVoyant analyzed the existence of DNS-based email security protocols across the 20 identified biotech and pharmaceutical companies - these are basic email security steps to prevent phishing attempts. BlueVoyant also looked for evidence of unsecured RDP ports.

The graph above shows that 77% of companies had both unsecured RDP ports and email domains lacking basic security measures. Almost 10% had unsecured RDP ports and no email security on their primary corporate email domain. Only three companies had secured their remote desktop protocols and secured their email.

These companies may use endpoint security devices or other defenses to help protect against phishing attempts, in particular - but the lack of basic security protocols (securing ports, email security) across these two different vulnerable points suggests an industry that has more to learn from the devastating mistakes of the last three years.

[7] https://www.coveware.com/blog/dont-become-a-ransomware-target-secure-rdp
[8] https://www.carbonite.com/blog/article/2019/08/ransomware-preys-on-smbs-via-rdp-attacks-spam-emails

CYBER THREATS AND COVID-19

The largest companies had the most malicious traffic. The bigger they were, the more attackers knew about them.

BlueVoyant also sought to examine how COVID-19 had changed the landscape for pharmaceutical companies.

Eight companies emerged as leaders in the race for the COVID-19 vaccine. The companies varied enormously in size and profile - ranging from established giants such as Johnson & Johnson to relative unknowns such as NovaVax. This allowed BlueVoyant analysts to examine whether COVID-19 had substantially changed the risk profile for pharmaceutical companies. Did being a competitor in the vaccine race make companies more at risk from attack? Was there evidence of any insidious COVID-19-related threats that were novel?

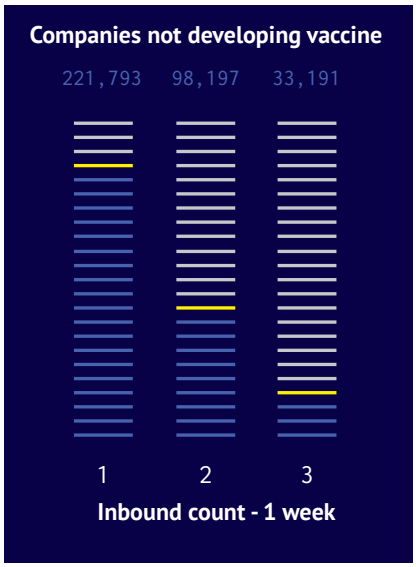
The first clear outcome related to threats: companies developing the vaccine faced a much larger volume of threats, both in total number and proportionally, than companies not in the race.

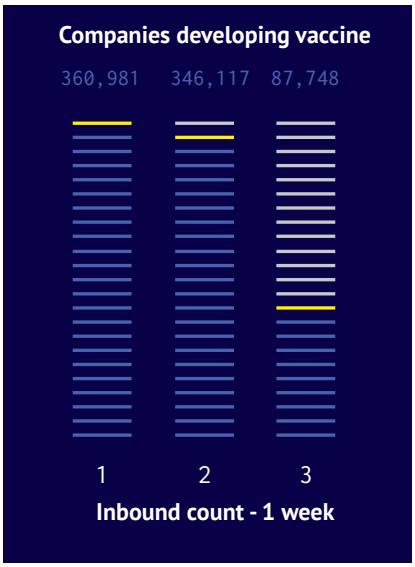
Sometimes, this discrepancy was striking. The table below shows the top companies by the number of observed inbound malicious events - the top three companies not developing a vaccine versus the top three companies developing one. For companies not developing a vaccine, the trend was clear: the largest companies had the most malicious traffic. The bigger they were, the more attackers knew about them.

For companies developing a vaccine, not only did they show a much larger count in total - but they were smaller companies. The single largest count observed was found targeting a company frequently in the news but smaller by an order of magnitude than most other companies in the list.

The list of eight companies as of summer 2020

1. GlaxoSmithKline
2. Pfizer
3. AstraZeneca
4. Johnson & Johnson
5. NovaVax
6. Moderna
7. CanSino
8. Sinovac





Attackers are focusing on companies developing a vaccine. This is certainly clear for nation-state attackers - but the sheer volume of traffic observed by BlueVoyant suggests that other actors, including the criminal and the merely opportunistic, are coming for them as well.

In addition to the heightened threats against companies developing the vaccine, BlueVoyant also observed novel coronavirus-related threats facing all of the companies analyzed.

DOMAIN	KNOWN FOR	HOW MANY CO'S AFFECTED
Corona.webcam	Phishing	1
Coronavirus-support-group.co.uk	Phishing	1
Covid19vaccinetrial.co.uk	Malware (now legitimized)	2
covsafe.uk	Suspicious activity	1
Covid-monitor.org	Phishing	1
Covidguide.health	Phishing (now legitimized)	2

The table above lists known malicious domains that were observed in traffic coming from four companies, in signs of compromised devices or networks. When BlueVoyant analysis observes traffic from a company's network space reaching out to malicious domains, that suggests that an employee's device downloaded malware through a phishing link (or, less likely but still possible, that a device was compromised by remote methods).

In a previous report[9], BlueVoyant identified the rise of COVID-19-related domain registrations in the first few weeks of the pandemic. Many of these were opportunistic; many others were outright criminal. The above domains match the signs of this surge in malicious infrastructure: the domains that were all registered in early March 2020 were early flagged for phishing activity (and at least once for being associated with known malware). It also appears that they infiltrated pharmaceutical networks.

Domains that were all registered in early March 2020 were early flagged for phishing activity

[9] https://www.bluevoyant.com/blog/attack-vectors-using-covid-19

CONCLUSION AND RECOMMENDATIONS

BlueVoyant analysis has confirmed an increasingly dangerous threat landscape for biotech and pharmaceutical companies. These companies, already prime targets for opportunistic criminals and nation-state actors alike, face an even more elevated risk environment in the current pandemic. Attacks on biotech and pharmaceutical companies are on the rise. All biotech and pharmaceutical companies face high volumes of threat actor activity, much of it sophisticated and targeted. Those companies identified as leading in the race for the COVID-19 vaccine face substantially higher levels of threat actor activity.

While these companies face higher levels of risk than ever before, many are still not securing their systems adequately against their most common threat: ransomware attacks. Specifically, many of these companies are notably weak in the areas of:

- Vulnerability and Patch Management
- Basic IT Hygiene and Best Practices for limiting exposure

In a time when more employees are working from home, the exploitation of remote work environments by ransomware groups is going to lead to more damaging intrusions.

With critical industries, it is incumbent on corporate leaders to prioritize cybersecurity - as much for the success of their companies and their critical data and IP as for their customers and clients. Biotech and pharmaceutical are critical sectors, now more than ever, and risks to IP cannot be mitigated through litigation with today's nation-state and cyber criminal threats. Biotech and pharmaceutical companies must move away from the academic mindsets of allowing open computing for researchers, moving towards a culture of security-first.

Companies should review... their Board and C-suite oversight of their cybersecurity program. Questions that need to be answered include:

- What prioritization and cyber protections are in place for their own data assets? For key manufacturing processes?
- How many collaborators in R&D and manufacturing hold sensitive data or operate critical processes? How well are those partners/vendors protected?
- How familiar is the Board/C-suite with the cyber risk management plan? What level of cybersecurity does it provide? What financial or capability trade-offs were made in setting the plan? What metrics and reporting processes are in place to provide sufficient regular oversight?
- How well developed are resiliency and recovery plans? How recently was a serious attack and recovery simulated?

CIOs and CISOs should review... the effectiveness of their programs, and forward looking multi-year plans. Questions that need to be answered include:

- Is the cyber defense posture currently at the right level considering the business value at risk, the financial resources that can be effectively spent, the cyber capabilities available, and likely attacker activities?
- Is there a multi-year plan in place to take cyber defense to the desired level that has been shared with and signed off by the C-suite/Board?
- Do the endpoint and network protection programs demonstrate competency against the advanced TTPs across a comprehensive framework like MITRE ATT&CK®?
- Is there an effective company-wide cyber hygiene and patching program in place with effective metrics and visibility?
- Are there training and testing programs in place to drive employees (including scientists and researchers) to the behaviors needed for strong cybersecurity?

Lastly...

companies must continuously monitor for and address new attack vectors. Importantly, once a company has secured its own systems, it needs to look outward to supply chain security. Biotech and pharmaceutical companies, more than most industries, are in tight and varied webs of supply chain dependencies – with links across manufacturing and distribution, healthcare, and data centers and tech providers. Supply chain security is a critical step in ensuring adequate security against third-party risk.

BlueVoyant

CONTACT THE TEAM

Contact Us
BlueVoyant Headquarters
335 Madison Ave, Suite 5G
New York, NY 10017

Tel: 00 (1) 646-558-0052 (8-5 EST)
Email: contact@bluevoyant.com
www.bluevoyant.com