INTSIGHTS
A RAPID7 COMPANY

Building Immunity:

The 2021 Healthcare and Pharmaceutical Industry Cyber Threat Landscape Report

Table of Contents

Introduction

A Unique Risk Profile

The healthcare and pharmaceutical industry has a complex and challenging cyber threat landscape. In 2020, more large healthcare data breaches were reported than in any other year. In addition, 2021 has seen five consecutive months (March through July) in which industry data breaches have been reported at a rate of two or more per day. Incidents of ransomware are also sharply increasing over time.

Certain operational and compliance requirements placed on healthcare organizations give them a unique risk profile and often leave their attack surfaces more vulnerable to compromise. Key features of this industry's distinctive risk profile include: a common emphasis on usability over security and a lower tolerance for downtime; compliance-driven approaches to security; and the greater vulnerability of medical devices. The health and security implications of the COVID-19 pandemic have also exacerbated many preexisting risk factors within the industry.

Valuable Data Stores

The data and credentials associated with healthcare organization IT networks are widely available for sale on underground criminal forums. Criminals can use these forums to purchase unauthorized access to networks of compromised healthcare organizations, a phenomenon that facilitates ransomware attacks in particular. Hospitals and other healthcare providers have become top targets for ransomware operators due to their perceived and actual vulnerability to compromise and extortion. Patient records, a form of protected health information (PHI), are valuable commodities for sale on underground forums due to their high level of utility in identity theft operations. Health insurance details are also useful for insurance fraud.

Patient records are useful to state-sponsored threat actors for the same reason that criminals value them; they typically contain more detail than sources of personally identifiable information (PII) from other industries. Foreign governments can use patient records in support of intelligence operations, as in the case of the attack on Anthem by state-sponsored Chinese actors, one of the largest incidents to affect the healthcare and pharmaceutical industry.

Organizations in this industry, particularly pharmaceutical companies and potentially medical device manufacturers, possess high-value intellectual property that threat actors seek to steal. In particular, COVID-19 vaccines and treatments, as well as supporting research, have become high-priority targets for state-sponsored cyber espionage groups around the world, as governments struggle to vaccinate their populations and providers treat the growing numbers of the infected.

About This Report

The healthcare and pharmaceutical industry is a target for both criminal and state-sponsored threats. This report aims to map the broad contours of that threat landscape, with an emphasis on its most distinctive features and recent developments.

The report draws heavily upon IntSights' original coverage of underground criminal forums, which we provide to customers on an industry-specific basis via our threat intelligence platform (TIP), for source material to illustrate key points. We have supplemented this coverage with information from other sources, such as media and vendor reporting on state-sponsored attacks. This underground forum coverage sheds light on the data sets and accesses that criminals seek, and the various ways of monetizing them in the underground criminal economy.

Organizations in the healthcare and pharmaceutical industry can use this knowledge of their threat landscape — and the most relevant vulnerabilities — to take specific steps to improve their defenses against the particular types of threats that are most likely to affect them. We have included a recommendations section in this report to provide additional industry-specific guidance.

Distinctive Features of the Industry's Threat Landscape

Usability and Cybersecurity Are At Odds

Organizations in any industry must strike a balance between security on one hand and usability on the other. The varying business and operational needs of organizations in different industries are major factors in where and how they strike that balance. For example, the financial services industry is among the most security centric, given its high desirability as a target for criminals and its critical need for high levels of customer trust. It thus tends to strike that balance more heavily in favor of security.

In contrast, the frequently time-sensitive or urgent nature of clinical services at many healthcare providers sometimes leads them to strike that balance more in favor of usability. Security measures can be inconvenient, time-consuming, or disruptive to business operations, ranging from the few seconds needed to input multi-factor authentication (MFA) to the hours or more of downtime that it may take to patch a vulnerable device.

Healthcare providers that face life-or-death situations with their patients may have lower tolerance for interruptions, downtime, or inconveniences that could slow their ability to respond to urgent or time-sensitive clinical needs. The cost of such an emphasis on expediency is that it can leave organizations with more vulnerable attack surfaces. Combined with the high value of certain types of healthcare data, these vulnerabilities make these organizations more attractive targets to threat actors.

Compliance and Regulation Stops Short

The healthcare and pharmaceutical industry is heavily regulated in ways that have significant security implications. Compliance with the security standards of healthcare laws and regulations is a necessary but insufficient condition for a robust security posture. While it is both important and beneficial to check those security compliance boxes, a box-checking mentality can become counterproductive if it leads organizations to become complacent in a false sense of security, or to refrain from considering and defending against threat scenarios that security compliance standards did not envision.

Healthcare organizations should treat the industry's security standards as a bare minimum and seek to go above and beyond what they require. Attackers will probably not abandon an attack simply because their target is security compliant; rather, they will simply find other ways to achieve their goals that the legal or regulatory security requirements do not cover. Laws and regulations also generally do not keep pace with the much faster evolution of the threat landscape and the tools and tactics that attackers use. These compliance and regulation requirements are thus at risk of becoming dated and less effective against new types of attacks.

Breach notification requirements, such as those from the US Health Insurance Portability and Accountability Act (HIPAA), cannot only increase the costs of data breaches but may also make healthcare organizations more desirable targets for a specific form of extortion, at least in the eyes of criminals. The ultimate costs of a patient data breach for US healthcare organizations can include the cost of notifying affected patients and, in some US states, providing credit monitoring services to protect them against identity theft.

Criminals are aware of these breach-related costs, and many believe that healthcare organizations are more likely to comply with data disclosure extortion demands out of a desire to avoid these costs. Threats to disclose compromised data, rather than simply encrypting it for ransom, are now a standard component of ransomware attacks. Ransomware operators follow through on these threats by posting files from ransomware victims on dark web pages where they are accessible to other criminals for their own malicious purposes.

Ransomware data dumps are "a gift that keeps on giving" in the sense that they enable other attackers and fraudsters to continue exploiting the victim beyond the original attack. For example, the inclusion of credentials or network reconnaissance maps in these data dumps could facilitate future attacks by other actors unrelated to the original attackers. Other fraudsters could also use disclosed HR records or customer or patient data for identity theft or other forms of fraud.

Vulnerable Medical Devices Increase the Risk of Compromise

Other regulatory requirements may have indirectly and inadvertently resulted in the weakening of healthcare organizations security postures by leaving medical devices vulnerable. For example, the US Food and Drug Administration (FDA) requires medical device manufacturers to **submit new 510(k) requests** for FDA approval of "significant" modifications to previously approved devices. The FDA has indicated that updates to medical devices for purely security reasons typically do not meet this threshold. There has nonetheless been sufficient ambiguity as to what modifications are "significant" enough to require new approval that some manufacturers have been discouraged from issuing security updates. Out of an abundance of regulatory caution, or perhaps a spirit of "overcompliance," some manufacturers may have hesitated to issue security updates for their medical devices if they believed that the changes might have met the 510(k) threshold and thus risked either noncompliance or a lengthy approval process.

As of this writing, the FDA is **pursuing reforms** that would actually require medical devices to effectively support security updates. Many medical devices are difficult to update, either because of their design or the ways in which healthcare organizations deploy them. In addition, medical devices may receive less security support from their end users when they deploy them outside the defensive perimeters of their conventional information technology (IT) networks. Legacy medical devices pose even greater vulnerability risks. They may be unsupported or rely on unsupported operating systems, and thus not receive security updates for new vulnerabilities. Many of these medical devices have long lifespans of a decade or more, allowing them to remain vulnerable for longer periods of time than conventional IT devices. Vulnerable medical devices can serve as initial access points, persistence mechanisms, or enablers of lateral movement in attacks on the networks of hospitals and other healthcare providers.

Healthcare Organizations Have Non-Health Systems Too

Security professionals on the in-house security teams of organizations in various sectors often focus on threats specific to their respective industries, such as healthcare, financial services, or oil and gas. This focus is well founded; many threats are industry specific, and healthcare in particular has a very distinctive risk profile. Nonetheless, a focus solely on one's own industry can often obscure the relevance of threats seen as primarily affecting organizations in other industries.

For example, like many other consumer-facing organizations, healthcare organizations accept credit cards for payment, either in person or through various online or mobile variations. This data and the attack vectors need to be protected as well as PHI is protected. The various attack surfaces and vulnerabilities need to be understood and addressed, preferably in conjunction with the protection of PHI data. In a similar vein, the attack surface of medical device or pharmaceutical manufacturers may resemble those of industrial, manufacturing, or energy organizations, with industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems for the production of medical devices or pharmaceutical products.

Specific Threats in Healthcare and Pharmaceuticals

The COVID-19 Pandemic Challenges Traditional Security Protocols

The COVID-19 pandemic has caused a significant transformation of the threat landscape across all industries and their attack surfaces, but to varying degrees. The implications of this transformation for the healthcare and pharmaceutical industry have arguably been more profound.

If nothing else, the often large numbers of COVID-19 patients at many healthcare providers have placed additional burdens or strains on them and their resources that can impede their ability to handle security threats. For example, doctors and nurses at an overwhelmed COVID-19 ward may be more likely to open malicious attachments or links if they simply do not have time to scrutinize suspicious email messages.

The reduced tolerance for downtime that may make healthcare organizations more vulnerable to the extortion of a ransomware attack under normal circumstances may be even lower if they are overwhelmed with critical COVID-19 patients. Such pressures may make them more likely to decide to pay the ransom, making them more attractive targets for ransomware operators.

From a more technical perspective, the clinical requirements of responding to often large and sudden surges of COVID-19 patients may, in some cases, have left the attack surfaces of many hospitals more vulnerable. Rapid increases in demand for ventilators and intensive care units (ICUs) may have led some hospitals to add devices to their networks in ways that were even less secure than usual. Given the above-mentioned tendency of medical devices to leave a healthcare organization's attack surface more vulnerable, an increase in ventilators on a hospital's network in response to an influx of COVID-19 patients probably gives attackers more opportunities to compromise that network.

The strong sense of urgency behind COVID-19 vaccination campaigns was probably why ransomware operators targeted the health department of the Italian region of Lazio and disabled its COVID-19 vaccination booking system in August 2021, disrupting the scheduling of new vaccination appointments for days. Lazio includes the city of Rome and is one of Italy's most densely populated regions. The attackers probably believed that the Lazio health department would be more likely to pay ransom out of a strong desire to resume vaccination bookings as soon as possible, as well as growing public demand for vaccination in the wake of Italy's introduction of its "Green Pass" vaccine passport. There have been conflicting reports as to which ransomware family was involved in the attack, with sources identifying both RansomEXX and LockBit2.0 ransomware. RansomEXX, also known as Defray777, previously targeted the French health insurance company Mutuelle Nationale des Hospitaliers (MNH), which specializes in covering healthcare professionals. The attackers had reportedly gained access to the Lazio health department network by compromising the administrative credentials of an employee of LazioCrea, an IT services vendor supporting the regional government of Lazio. That vendor compromise yielded VPN access that enabled the attackers to compromise the health department.

In June 2021, the English-speaking underground criminal forum user "Mastiff" advertised and sold a database of the COVID-19 vaccination records of nearly 7.4 million Italians; inhabitants of the Lazio region constituted the majority

of individuals in samples of the data that the actor shared. The actor claimed they obtained the data within the past month and maintained access to the source of the data, which they did not plan to sell. The data included names, dates of birth, fiscal codes (the Italian counterpart of US Social Security numbers), street addresses, phone numbers, email addresses, and hashed passwords (see Figure 1). It is unclear what if any role Mastiff might have had in the subsequent ransomware attack.

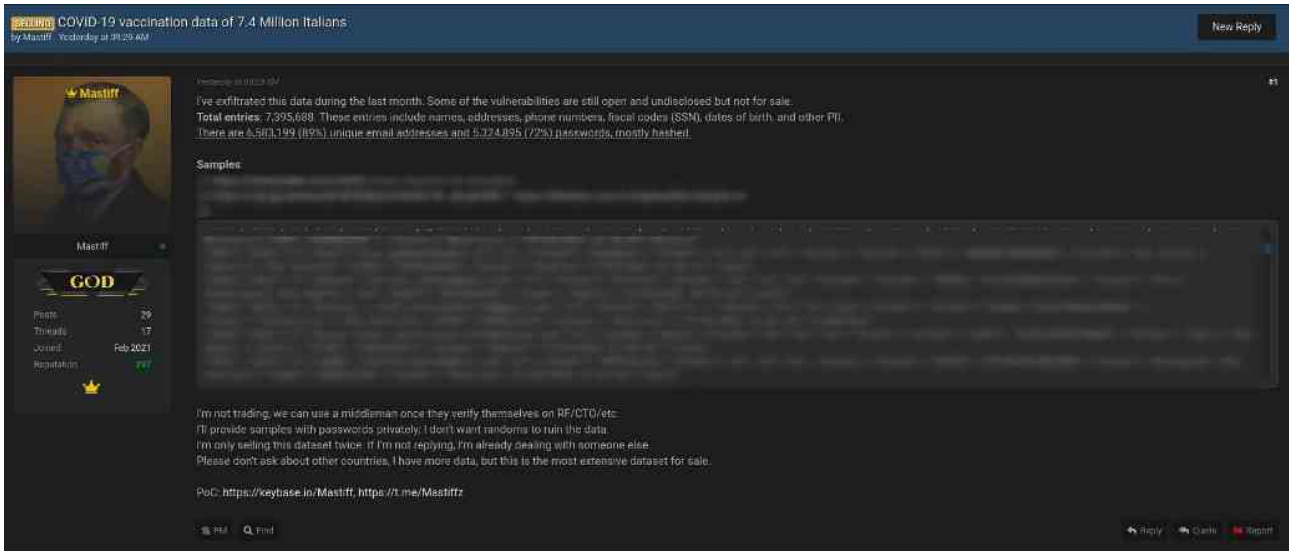


Figure 1

COVID-19 test results have also become a commodity on underground criminal markets. KelvinSecTeam, a South American criminal group, has increased its targeting of the healthcare sector during the COVID-19 pandemic in various ways. For example, it has become a vendor of compromised US COVID-19 test results. In October 2020, the group offered to sell 14,000 COVID-19 test results from a purported compromise of 360 Clinics, a network of clinics in Southern California. The database had fields for names, dates of birth, Social Security numbers, and health insurance details (see Figure 2). In February 2021, the same group offered to sell a database of more than 3,000 COVID-19 test results from a purported breach of Florida-based Delta Corps Diagnostics for $100 USD. The database included names, email addresses, passwords, dates of birth, phone numbers, street addresses, and identity documents (see Figure 3). Similarly, in March 2021, the underground criminal forum user "Research3r" offered to sell a database of 200 COVID-19 test results from the Russian city of Stavropol. The Russian-language database included fields for patients' PII (see Figure 4).

Figure 2

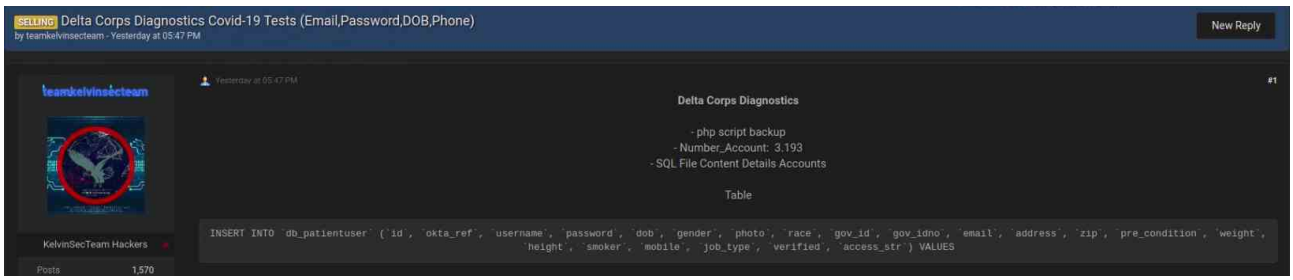


Figure 3

Figure 4

The COVID-19 pandemic has altered the attack surface of the healthcare industry by creating new patient data sets for attackers to target, including COVID-19 vaccination records and test results. The greater sense of urgency associated with these particular data sets may also make them more accessible or more desirable targets. The healthcare industry was already a desirable target because of the greater value and detail of its patient data, compared to PII sources from other industries. If a COVID-19 vaccination or testing record only contains a name and a date of birth, it is still useful to fraudsters, as dates of birth are a key ingredient in identity theft.

The growing adoption of or demand for digital "vaccine passports" and other ways of verifying COVID-19 vaccination or testing status at businesses, means of transportation, and other public places presents attackers with additional opportunities to compromise this patient data. Such pressures to show proof of vaccination are also creating a black market for compromised or fraudulent digital vaccination or testing records that "the willfully unvaccinated" or "the vaccine resistant" can use fraudulently in order to access public places and services in those jurisdictions requiring such proof, such as in Europe. In the United States, at least, there is already significant demand for **fake hardcopy vaccination documents**, as electronic documentation has not yet been widely adopted in most states, aside from New York and Hawaii.

IntSights threat intelligence shows there is a market in both the United States and in Europe for the production of fraudulent digital COVID-19 testing and vaccination documents. In many cases, these documents are being produced with the help of malicious insiders so that they appear legitimate upon verification. The malicious insiders have legitimate access to systems at COVID-19 testing and vaccination providers that generate genuine test results (see Figure 5) or record vaccination status. The malicious insiders can produce documents that withstand digital scrutiny, or they can even manually enter unvaccinated people into the vaccination registry so that they appear legitimate and can receive otherwise genuine vaccination records.

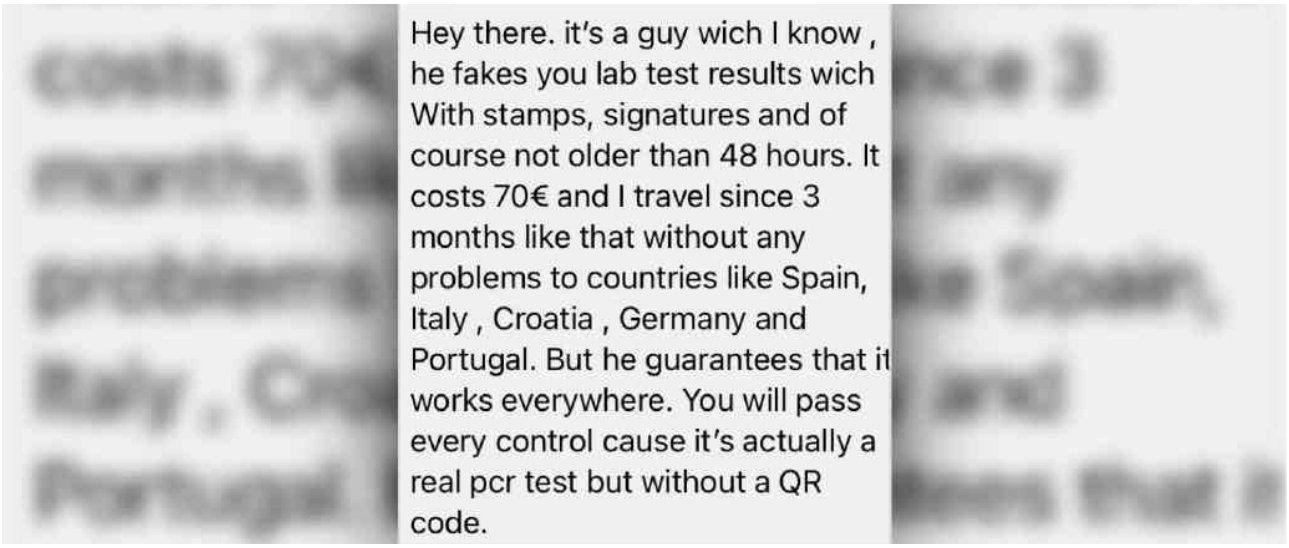


Figure 5

The COVID-19 pandemic led spam and phishing attackers to introduce much greater variety into the social engineering themes of their attacks. Many of them expanded far beyond their historic repertoire of stock, boilerplate themes like package deliveries and invoices to exploit the fear and uncertainty resulting from the pandemic. Many of these newer themes have been specific to the healthcare industry, such as COVID-19 tests and vaccinations or health insurance coverage. The proliferation of healthcare themes in spam and phishing campaigns increased the risk to healthcare organizations and their patients, who may be more likely to fall for these health-related social engineering themes and thus open malicious links or email attachments due to their greater relevance to the healthcare profession.

The rise of the remote workforce during the COVID-19 pandemic has transformed the attack surfaces and threat landscapes of all industries, but to varying degrees. Even though many healthcare professionals continued to work in person during the pandemic, any remote segments of healthcare organization workforces, perhaps in non-clinical support roles, make their attack surfaces more vulnerable. Home routers that employees use to connect to the internet are often vulnerable to compromise via weak or default passwords or vulnerable firmware. Compromised routers can enable further attacks on employees' connected endpoints, network traffic, or enterprise credentials. Employees working from personal devices without enterprise security software and often not compliant with best security practices are more vulnerable to compromise. For example, IntSights researchers covering the market for access to compromised computers discovered this sale of access to the home computer of a doctor who had transferred his practice's files to his personal computer. Such files are valuable to criminals seeking access to healthcare data for fraudulent purposes (see Figure 6).

Increased use of VPNs and the Remote Desktop Protocol by remote workers during the pandemic has also expanded the attack surface of many organizations and given attackers more opportunities to use this attack vector to gain access to enterprise infrastructure. The increased use of remote communication platforms, such as Zoom and Slack, has also given attackers more opportunities to send malicious links and attachments to remote workers and gain access to their private communications.

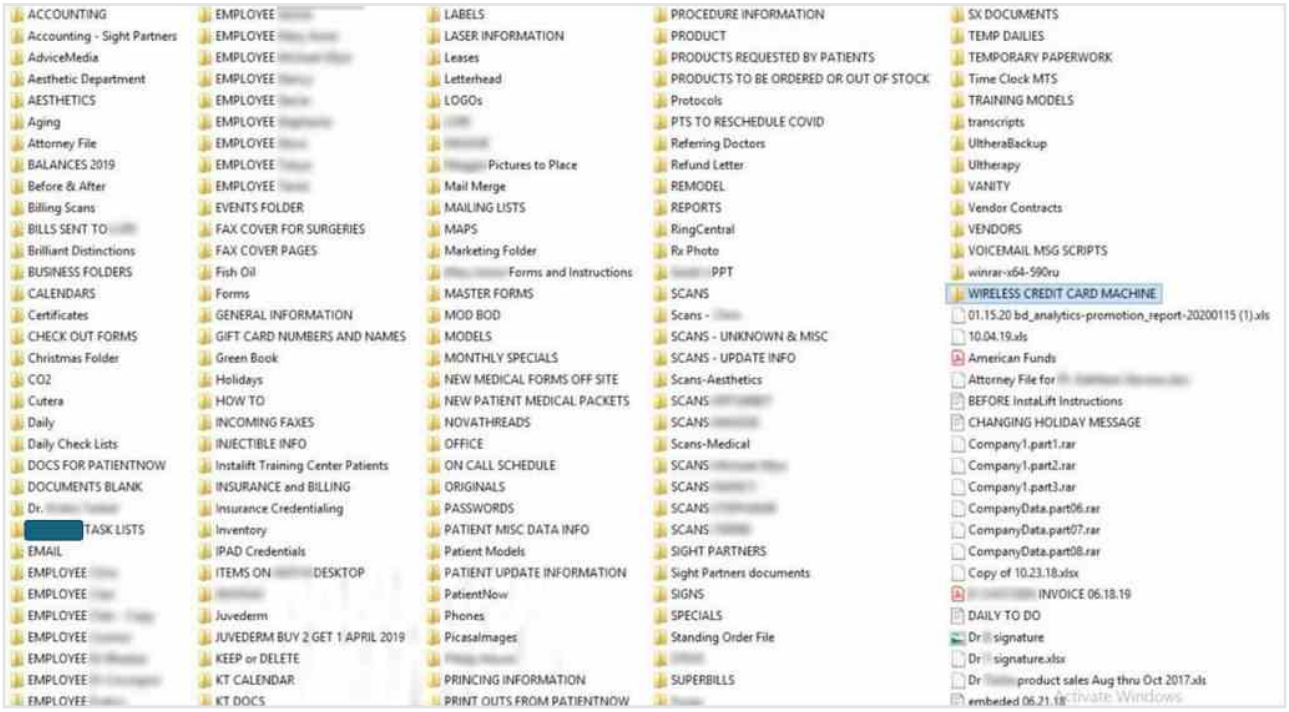


Figure 6

The COVID-19 pandemic also fueled the rise of telemedicine or telehealth services, in which healthcare providers treat patients virtually online. These services may reduce the risk of COVID-19 transmission by reducing in-person contact and allowing COVID-19 patients to remain in isolation, but they also increase the risk of cyberattack simply by giving attackers another target to compromise. The compromise of telehealth accounts and services can yield the data that criminals seek for various malicious purposes. For example, in April 2021, the English-speaking underground criminal forum user "fallensky519" offered to sell information from the user database of DocsApp, an Indian app that allows patients to consult with doctors remotely. The data purportedly included the names, usernames, passwords, email addresses, and phone numbers of more than 2,000 doctors and more than 7 million patients (see Figure 7).

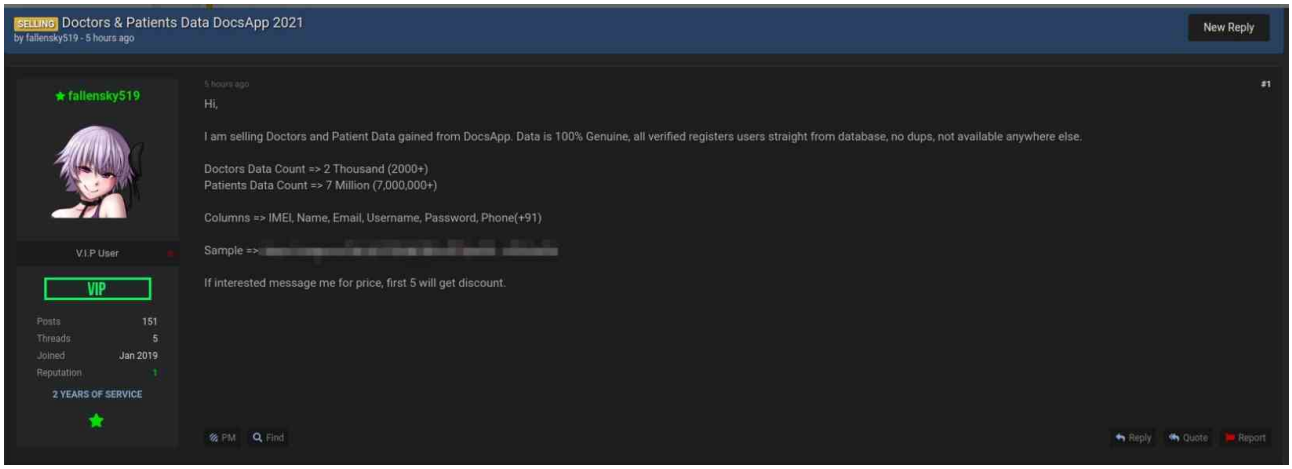


Figure 7

Pharmaceutical companies were desirable targets for intellectual property theft long before the COVID-19 pandemic, and they will likely continue to be victims of intellectual property theft long after the pandemic ends. The large research and development (R&D) investments of pharmaceutical companies in their products makes that intellectual property a high-value target for attackers.

The quest for COVID-19 vaccines and treatments, and the efforts of governments around the world to vaccinate their populations and treat the infected, has made these specific forms of intellectual property an even higher-priority target, particularly for state-sponsored cyber espionage groups. Pharmaceutical companies that produce or are developing COVID-19 vaccines or treatments, or healthcare providers collecting relevant data, are at an elevated risk of attack, as threat actors seek some of today's most highly coveted pieces of intellectual property worldwide. COVID-19 vaccines are important not only to protect one's own population, but for major powers like Russia and China to use as diplomatic or economic bargaining chips with developing countries.

It has emerged that all four of the most frequently covered state sponsors of cyber espionage — Russia, China, Iran, and North Korea — have targeted COVID-19 vaccine and drug treatment research and clinical trial data. The state-sponsored attackers identified thus far include:

- The North Korean Lazarus Group, responsible for the 2014 destructive malware attack on Sony Pictures Entertainment, subsequent financially motivated attacks on the SWIFT accesses of banks around the world, and other high-profile incidents
- The North Korean Kimsuky, which targeted the manufacturers of at least two COVID-19 vaccines that later received approval or authorization and have been widely used (Johnson & Johnson and AstraZeneca), plus Novavax, which, as of this writing, is waiting to seek approval for its vaccine
- The North Korean Bureau 325 of the Reconnaissance General Bureau (RGB), also known by security researchers as Cerium, which is less well documented but appears to have a special interest in COVID-19 research
- The Russian APT28, also known as Strontium and Fancy Bear, which was responsible for the 2016 attack on the US Democratic National Committee (DNC) and the subsequent impact of the disclosure of compromised email messages on the US Presidential election
- The Russian APT29, also known as Cozy Bear, which was responsible for the 2020 SolarWinds technology supply chain compromise campaign targeting primarily US Government agencies
- Unspecified Chinese actors that reportedly targeted Spanish research centers conducting COVID-19 vaccine research, according to Spanish officials
- Li Xiaoyu and Dong Jiazho, Chinese nationals that the US Department of Justice indicted for targeting companies conducting COVID-19 research, among others, on behalf of the Chinese Ministry of State Security (MSS)
- The Iranian Charming Kitten, which conducted a phishing attack against the US pharmaceutical company Gilead Sciences, the producer of the FDA-approved COVID-19 treatment drug Remdesivir

North Korea appears to be the highest-impact attacker in this area, with at least three groups participating in efforts to target at least three manufacturers of actually approved, authorized, or potentially approvable COVID-19 vaccines.

Controversy surrounding the vaccines, including widespread anti-vaccine sentiment, may also make vaccine manufacturers and public health organizations targets of hacktivist-style data disclosures. For example, in January 2021, there was a leak on the dark web of compromised data on COVID-19 vaccines from the European Medicines Agency (EMA), including discussions with the US FDA. The Russian-speaking actor that posted this information sought to cast doubt on the legitimacy of the COVID-19 vaccines (see Figures 8 and 9).

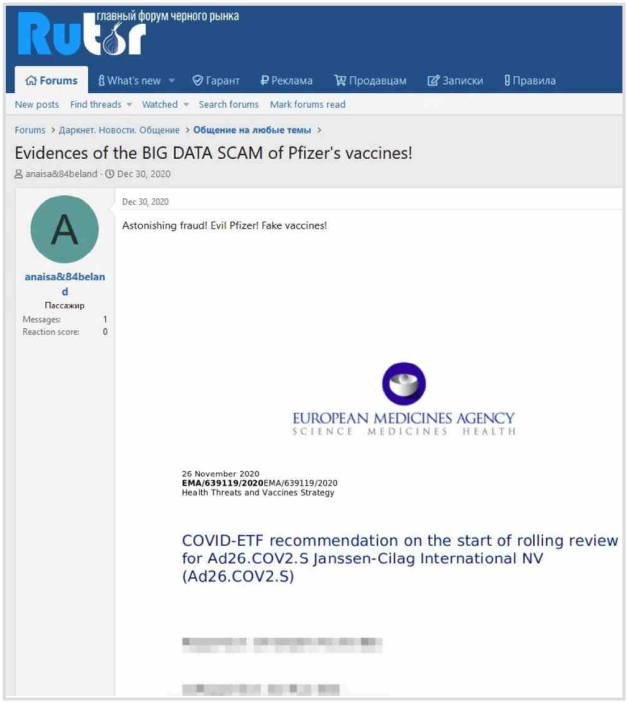
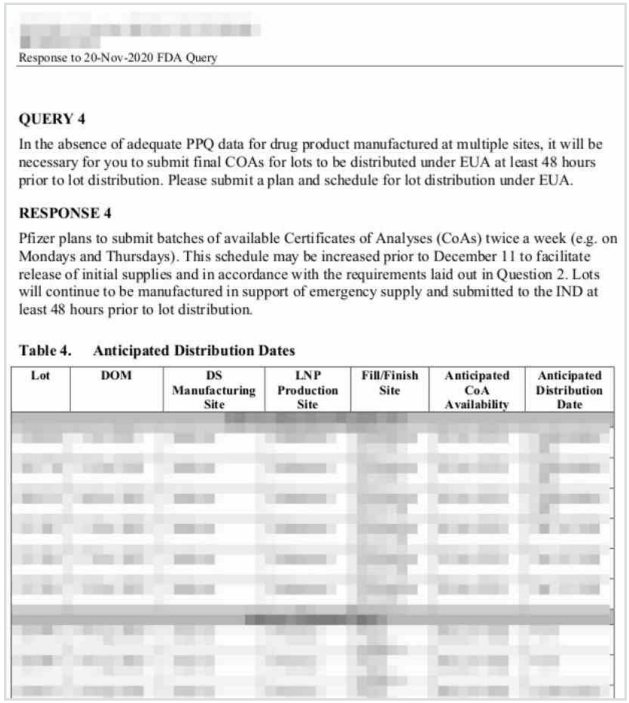


Figure 8


Response to 20-Nov-2020 FDA Query

QUERY 4

In the absence of adequate PPQ data for drug product manufactured at multiple sites, it will be necessary for you to submit final COAs for lots to be distributed under EUA at least 48 hours prior to lot distribution. Please submit a plan and schedule for lot distribution under EUA.

RESPONSE 4

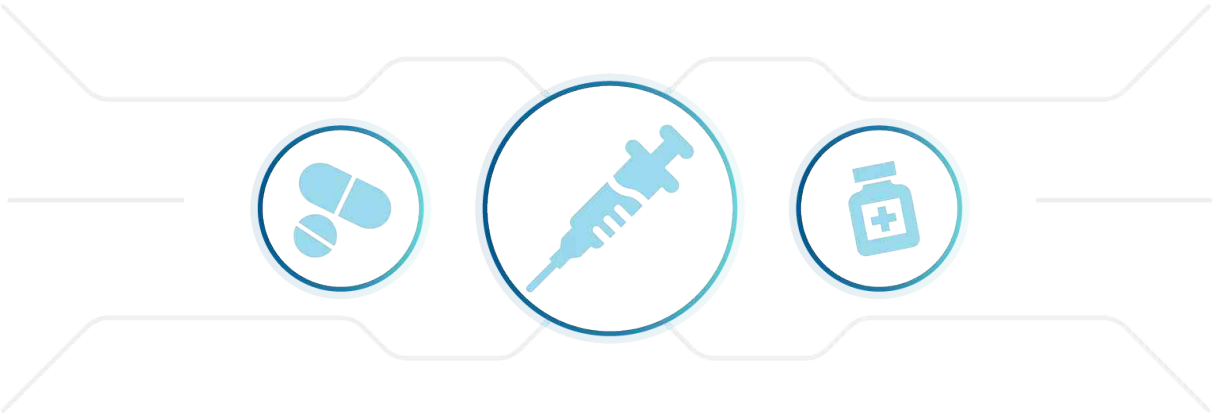
Pfizer plans to submit batches of available Certificates of Analyses (CoAs) twice a week (e.g. on Mondays and Thursdays). This schedule may be increased prior to December 11 to facilitate release of initial supplies and in accordance with the requirements laid out in Question 2. Lots will continue to be manufactured in support of emergency supply and submitted to the IND at least 48 hours prior to lot distribution.

Table 4. Anticipated Distribution Dates

Lot	DOM	DS Manufacturing Site	LNP Production Site	Fill/Finish Site	Anticipated CoA Availability	Anticipated Distribution Date

Figure 9

Opposition to public health measures against COVID-19 and the increased salience of public health organizations during the pandemic have made those organizations targets in their own right. For example, in July 2020, criminal forum username "3lv4n" offered to sell a database of 180,000 employees of the US Department of Health and Human Services (HHS), along with databases from technology and telecommunications companies. The listed HHS employees included those of the FDA, the Centers for Disease Control (CDC), and the National Institutes of Health (NIH). The database included employee names, titles, phone numbers, and email addresses.



Access to Compromised Healthcare Networks Is For Sale on Underground Forums

The COVID-19 pandemic and the associated rise of the remote workforce have also fueled the expansion and maturation of the sale of compromised enterprise network access on underground criminal forums. This black market for compromised network access predated the pandemic but grew dramatically in response to the increased opportunities that the pandemic and remote work created.

This phenomenon affects organizations in all industries, but, as a recent IntSights white paper demonstrates, healthcare organizations are among the most common victims of these sales. A data sample of these sales indicated that 19.5 percent of all observed victims were from the healthcare industry, which was tied for second place with financial services and energy and industrials. An analysis of the prices for these sales of unauthorized network access further indicated that pricing for healthcare organizations trends significantly lower than the cross-industry average of $9,640 and the cross-industry median of $3,000 USD. The average price for unauthorized access to healthcare networks was much lower at $4,860, with a similarly low median price of $700. The lowest observed price in the data sample, $240, was for access to the network of a healthcare organization in Colombia. Prices for healthcare organizations may trend lower due to the perception that they are easier to compromise (which may have an element of truth to it) or due to oversupply. Ransomware operators are a critical segment of the customer base for sales of compromised networks, where they deploy their ransomware payloads after purchasing access to them. The generally lower cost of buying access to healthcare organization networks has probably made them even more desirable victims for ransomware operators.

One of the most typical or "textbook" examples that IntSights researchers discovered was the sale of unauthorized access to a US regional hospital network in July 2020. The Russian-speaking seller, username "TrueFighter," offered a combination of RDP access and domain administrator credentials for $3,000 USD. Hospitals are popular targets for ransomware operators, who are also among the most frequent buyers of these network access sales. RDP is a common persistence mechanism that the initial attackers use to transfer the access that they are selling to their buyers, as in this case. Domain administrator credentials give buyers high privileges to execute ransomware payloads or achieve other malicious objectives. A thorough and efficient criminal would also probably exfiltrate patient data from this hospital network before deploying ransomware on it, as fraudsters would pay good prices to use this information in identity theft operations. The attacker might further threaten to disclose that compromised data on the dark web if the hospital refused to pay ransoms. The price of $3,000 USD for this sale was the cross-industry median price for the entire sample in the recent IntSights white paper and also the single most common price in the entire sample (see Figure 10).

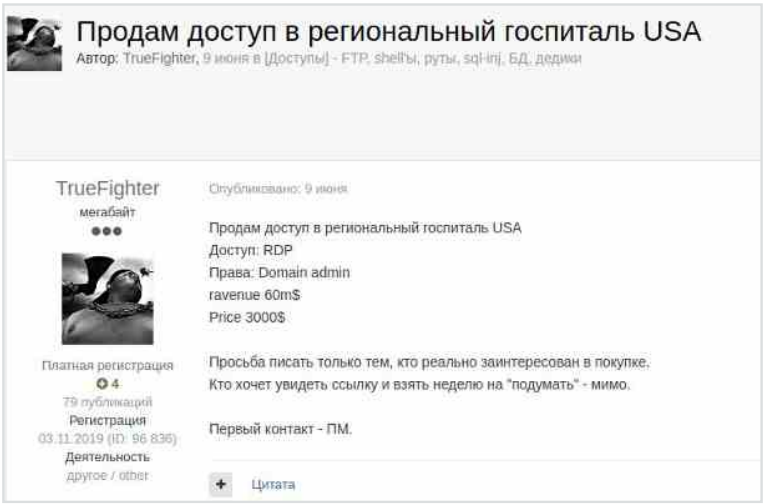


Figure 10

In another fairly typical example of these sales, the Russian-speaking criminal "hardknocklife" auctioned off RDP access to a US hospital in September 2020. They noted the value of access to patient records as a selling point for prospective buyers but indicated that they had no interest in this data themselves. Many criminals who specialize in selling intrusions that they initiated choose to do so because they recognize that it may be more cost-effective for them to turn over the monetization of a breach to others that specialize in relevant fields, such as identity thieves or ransomware operators. In other words, "hardknocklife" may have recognized that they could be more effective or profitable as a dedicated intruder than as an amateur fraudster or identity thief. The low price of $500 USD at which they started the auction suggested that they wanted to move this inventory quickly, but their higher "buy now" price of $5,000 USD also recognized the high monetary value of US patient records. In contrast to the hospital sale above, this offering did not include administrative privileges, which would probably limit how high of a price the seller could expect to receive. A lack of administrative privileges limits what an attacker can do on a network, and many ransomware payloads in particular require administrative privileges to run (see Figure 11).

Figure 11

In another example of Russian-speaking criminals targeting the US healthcare sector, criminal forum username "bl33d" auctioned off access to the network of an Illinois-based provider of home healthcare, nursing, and physical therapy services in October 2020. The bidding started at the relatively low price of $200 USD, increased in increments of $20 USD, and had a "buy now" price of $500 USD. Samples of data that the actor shared suggested that the breach would yield access to the company's financial data and patients' dates of birth, Social Security numbers, and health insurance details (see Figure 12).

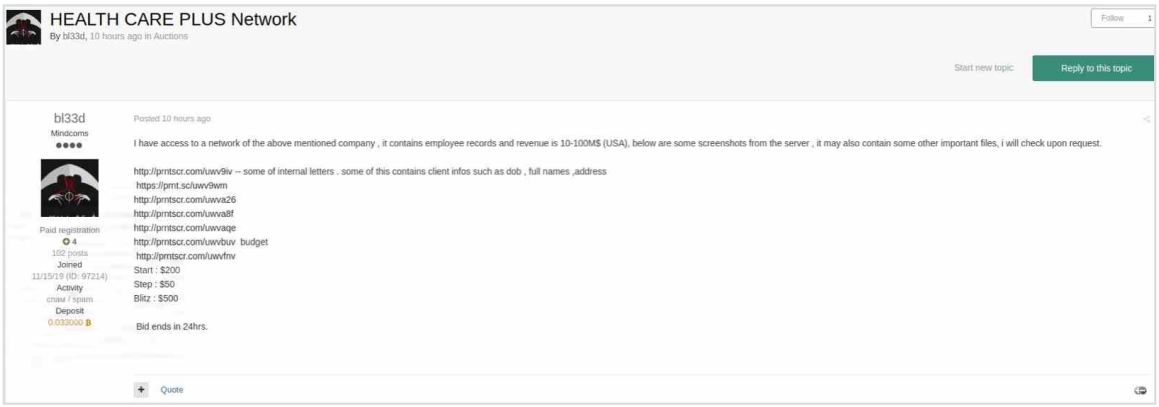


Figure 12

Compromises of healthcare organizations' public-facing web infrastructure, even without access to their internal networks, can also be useful to threat actors as a way to target and collect data on patients. For example, in March 2021, underground criminal forum username "hefaistos" auctioned off administrative access to the WordPress control panel of the website of a US-based network of approximately 60 healthcare clinics. The bidding began at $500 USD and increased in increments of $200 USD. Prices for unauthorized access to web infrastructure are typically lower than those for internal network access (see Figure 13).

Figure 13

The healthcare industry in the United States is a top target for criminals, as is the case across most other industries, because the US has a large and wealthy economy, and because its use of English, the world's leading lingua franca, makes US victims more readily accessible. Healthcare organizations in other countries, particularly affluent ones with large economies, can also become targets. For example, in November and December 2020, criminal forum username "Cipher_Strike" offered to sell unauthorized access to the networks of two healthcare organizations in the United Arab Emirates (UAE): Emirates Hospital and Vidal Health (see Figures 14 and 15, respectively). Similarly, in July 2020, the criminal forum user "drumrlu," who specializes in the sale of compromised enterprise networks, sold access to the network of a German group of hospitals in Saudi Arabia for $3,500 USD (see Figure 16).

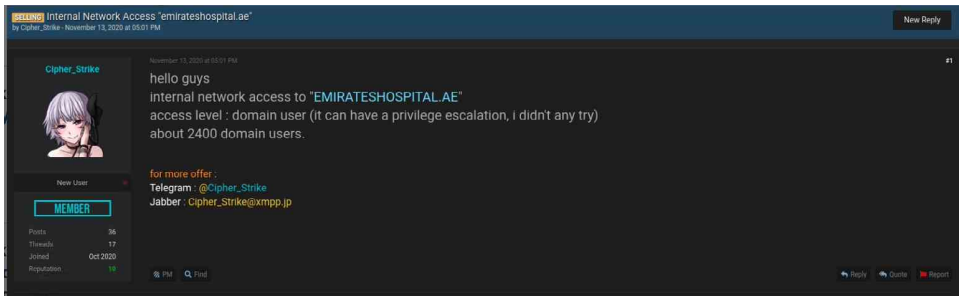


Figure 14

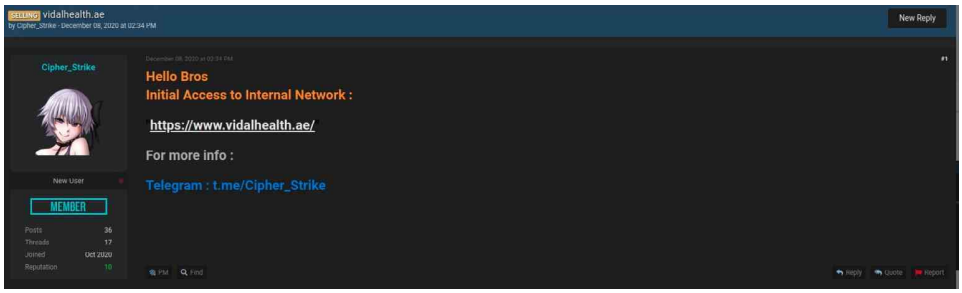


Figure 15

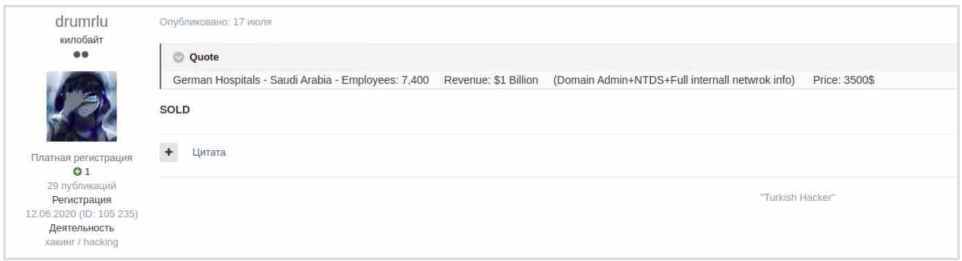


Figure 16

This preference for targets in affluent countries nonetheless fails to discourage criminals from targeting organizations in developing countries as well. For example, username "WebFluzzer" offered to sell administrative access to and data from the website of a Colombian healthcare organization for a grand total of $240 US (see Figure 17). All other things being the same, prices for victims in developing countries tend to be lower, as in this case.

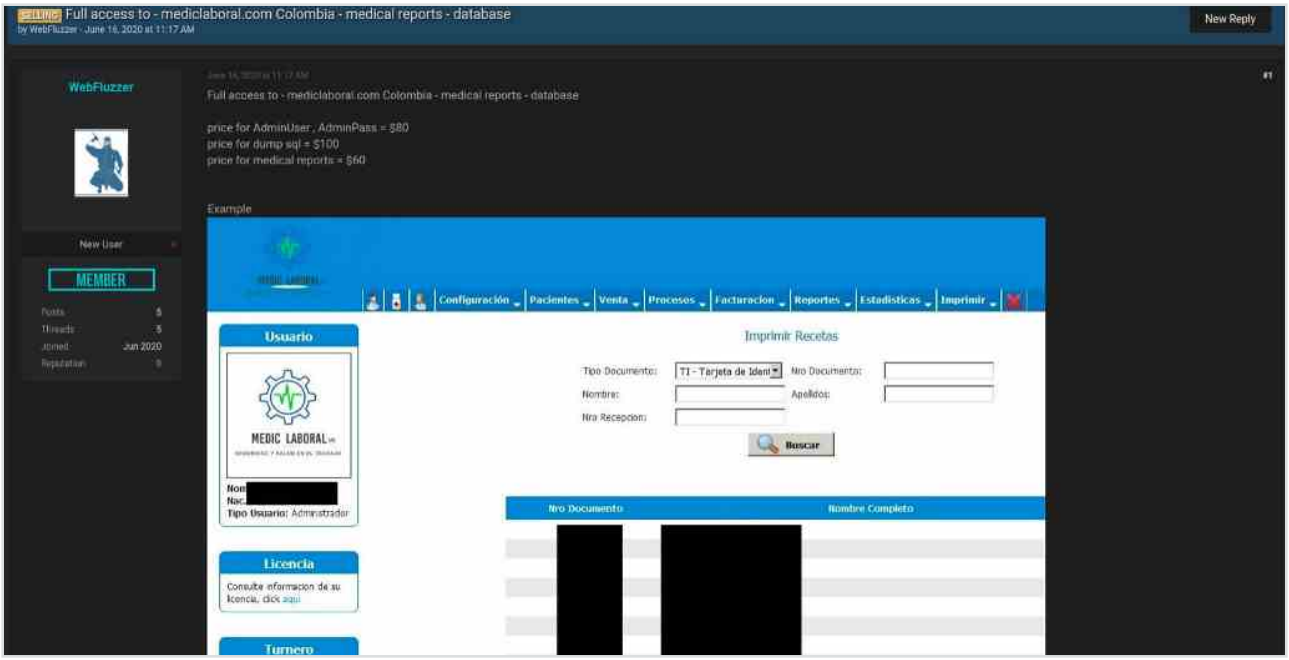


Figure 17

Ransomware Has a Foothold in the Industry

The popularity of healthcare providers in general and hospitals in particular has been an enduring and well-documented feature of this industry's threat landscape since at least 2016. The network access sales described thus far have, however, become significant enablers for ransomware attacks across all industries, including healthcare. Ransomware operators represent a significant portion of the customer base for this niche market. The below-average cost of access to the networks of healthcare organizations has probably made them more attractive targets to ransomware operators than they already were before this market for unauthorized network access sales matured in the past year and a half.

The May 2021 Conti ransomware attack on Ireland's Health Service Executive highlights the implications for healthcare providers of a newer facet of ransomware attacks that has become a standard feature of most of them, across all industries, in the past year or two: the threat of data disclosure. In addition to encrypting files and holding them for ransom, ransomware operators now routinely threaten to disclose compromised information, usually on dark web sites established specifically for this purpose, if victims refuse to pay ransoms. The goal of this tactic is to increase pressure on victims to pay ransoms and to undermine the value of backups as a defense against ransomware attacks. In the case of the Conti attack on the HSE, the attackers demanded $20 million USD in exchange for not disclosing compromised HSE data, including patient records. Such data disclosures are harmful to organizations in any industry, but the exposure of healthcare provider patient records poses the further complications of compliance violations, legal issues, breach notification costs, and the long-term risk and enduring effects of identity theft for exposed patients.

IntSights' coverage of ransomware data disclosures and threats indicates that Conti ransomware operators in particular have been among the most prolific practitioners of this specific extortion strategy against healthcare providers. Identifiable healthcare victims of Conti ransomware data disclosures in the past year include: California-based Empire Physicians Medical Group in May 2021; Laura Daniela Emergency Integral Clinic in Valledupar, Colombia in March 2021; New Mexico-based Rehoboth McKinley Christian Health Care Services in February 2021; Virginia-based TaylorMade Diagnostics and Nevada-based Gastroenterology Consultants in January 2021; HT Medica, a Spanish network of diagnostic imaging centers, in December 2020; Miami-based Leon Medical Centers, also in December 2020; and Higginbotham Family Dental in Arkansas and Tennessee in September 2020.

These data disclosures typically include a combination of patient and financial data. In the case of Leon Medical Centers, the actors started by disclosing financial data and then threatened to publish patient records, including Social Security numbers, health insurance details, home addresses, patient photos, diagnoses, and treatment plans. The actors blamed Leon Medical Centers for their allegedly poor security (see Figure 18).

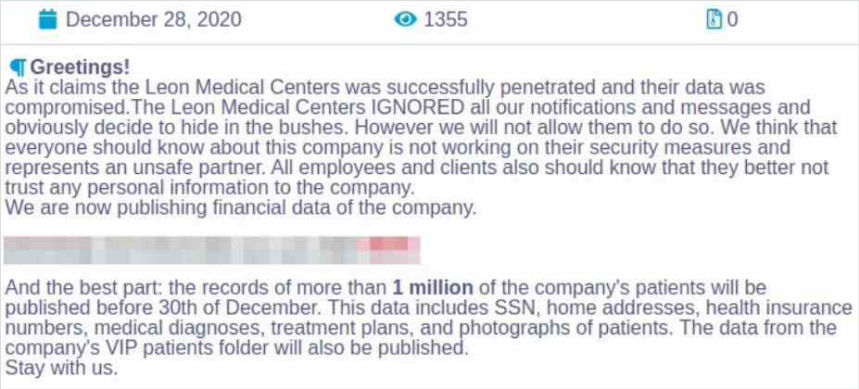


Figure 18

More broadly, security vendor statistics indicate that the healthcare and pharmaceutical industry was the fourth-most frequent target of Conti ransomware attacks as of early 2021, and that Conti was the second-most frequent ransomware family to target this industry in 2020; only the now-defunct Maze ransomware targeted healthcare and pharmaceutical more frequently last year. Conti's targeting of healthcare providers and other first-responder organizations in the US was severe enough to prompt the FBI to issue a **cybersecurity alert** about Conti's targeting of these organizations in May 2021. Conti evidently targeted other first-responder organizations for the same reason that ransomware operators in general have targeted healthcare providers: the perception that the time sensitivity of their services and their lower tolerance for downtime make them more vulnerable to extortion.

In contrast to many other ransomware operators, Conti actors evidently do not care about maintaining their reputation for integrity in dealing with their victims, as they have a track record of breaking their word, according to incident responders. There are several reasons why ransomware victims might choose to not pay ransoms, one of which is that deceptive ransomware operators may fail to uphold their end of a deal; they may simply accept ransom payments without decrypting encrypted files, or they may sell or disclose compromised data that they agreed to protect. Conti operators are reportedly more prone to this type of behavior.

Conti ransomware operators are not the only ones that have demonstrated their willingness to expose patient records as part of a data disclosure extortion attempt. For example, in January 2021, "NetWalker" ransomware operators disclosed patient records and other files that they claimed to have obtained from a breach of Christies Beach Medical Centre in Australia (see Figure 19).

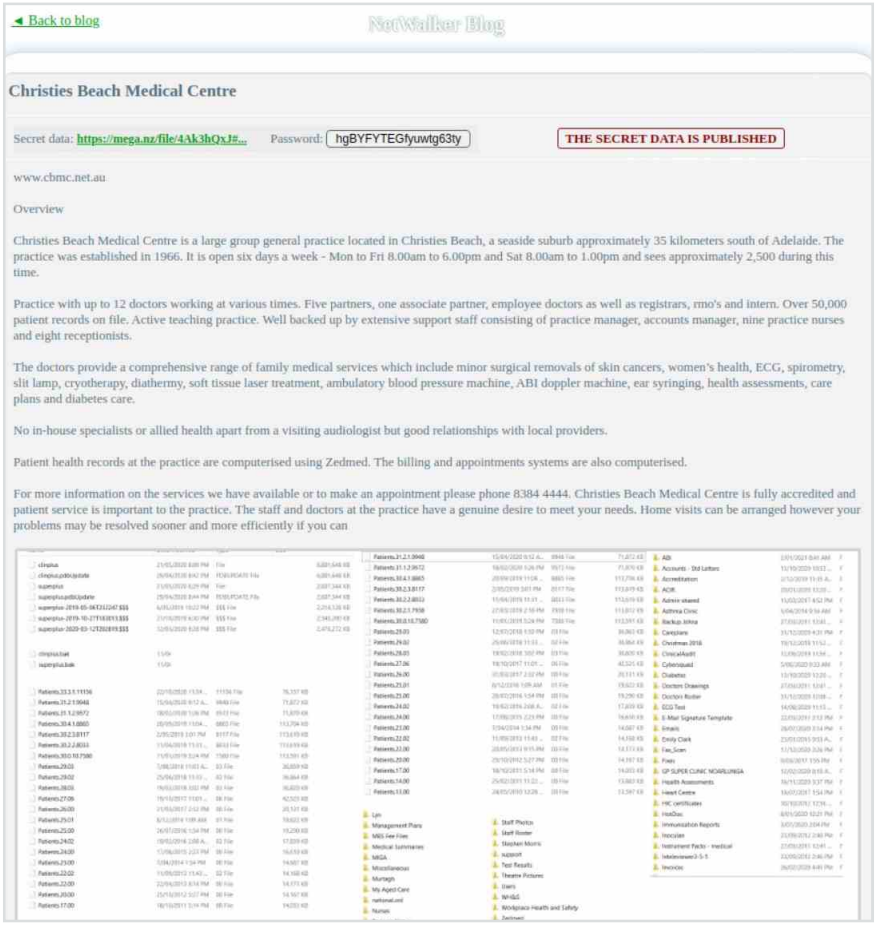


Figure 19

Despite the justifiable focus of many healthcare security professionals on protecting PHI and a desire to avoid PHI compliance violations as a result of ransomware data disclosures, it is also possible to do significant damage to a healthcare organization simply by exposing its financial and other non-clinical business information. For example, in April 2021, "Marketo" ransomware operators disclosed data that they claimed to have obtained from a breach of Absolute Dental, a network of dental offices in Las Vegas, Nevada. The leaked information was almost entirely financial or contractual in nature, including financial statements, accounting, tax payments, claims, contracts, and non-disclosure agreements (NDAs). The attackers attributed the breach to Absolute Dental's allegedly poor security hygiene and warned that it faced the risk of reputation damage for its alleged negligence (see Figure 20).

Figure 20

Healthcare providers are not the only targets of ransomware in this industry. In February 2021, operators of the DarkSide ransomware affiliate program disclosed more than 1TB of financial and technical data that they claimed to have obtained from a breach of the UAE-based Amico Group, a supplier of medical devices. The compromised data reportedly included bank accounts, including credentials and balances; details on cash dividends and cash-outs; financial details on the company's CEO, including bank statements and jet rentals; NDAs; HR and B2B contracts; price lists; more than 1,000 passwords for remote access to the company's infrastructure; network maps; backup details; the details of the network's Active Directory and domain controller database; contact information, identity documents, and other PII for employees, including senior leadership. This information could enable bank fraud against the company, identity theft against its employees, and further intrusions into the company's network (see Figure 21). **DarkSide is the same** ransomware affiliate program responsible for the May 2021 Colonial Pipeline incident.

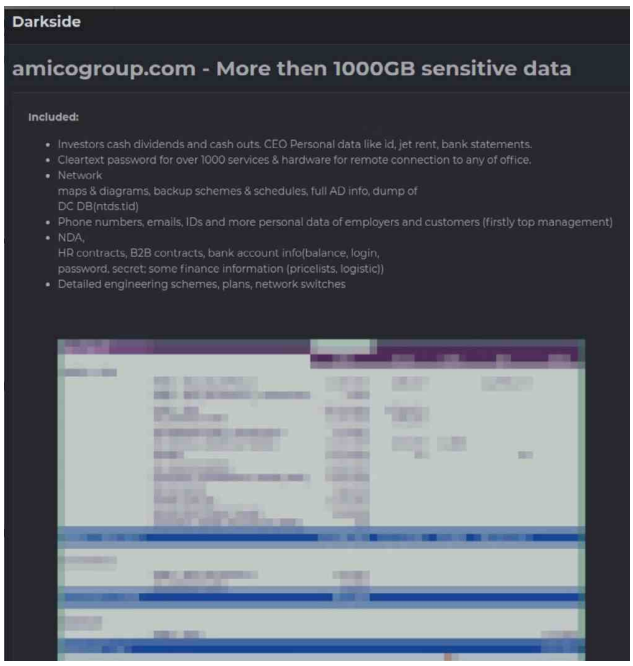
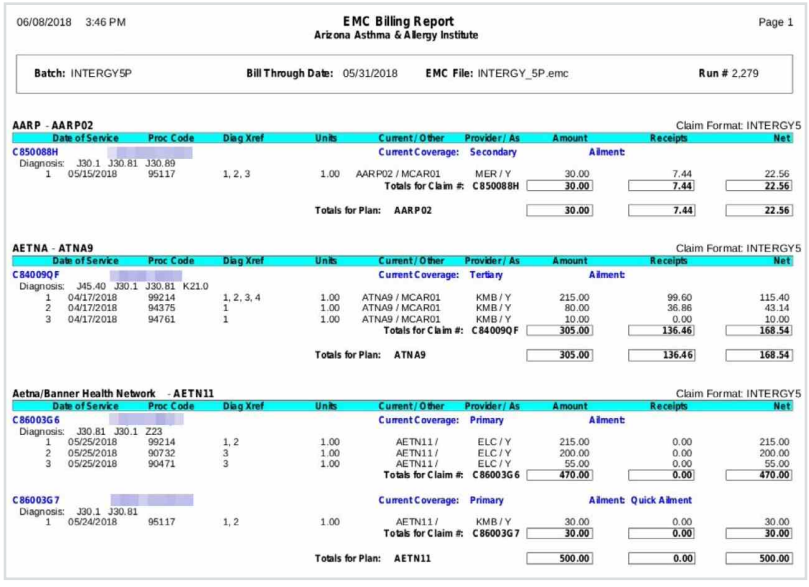


Figure 21

Other organizations that are not healthcare providers per se can become the sources of ransomware data disclosures of healthcare information. For example, in July 2020, Maze ransomware operators disclosed data that they claimed to have obtained from a breach of Medical Management, a healthcare practice management company. The compromised data included client billing documentation (see Figure 22). Similarly, in July 2020, NetWalker ransomware operators disclosed data that they claimed to have obtained from a breach of a New York City law firm that specializes in medical malpractice and personal injury cases. The disclosed data included email communications with attorney-client privileges.



06/08/2018 3:46 PM — **EMC Billing Report** — Arizona Asthma & Allergy Institute — Page 1

Batch: INTERGY5P Bill Through Date: 05/31/2018 EMC File: INTERGY_5P.emc Run # 2,279

AARP - AARP02 — Claim Format: INTERGY5

Date of Service	Proc Code	Diag Xref	Units	Current / Other	Provider / As	Amount	Receipts	Net
C850088H				Current Coverage: Secondary		Ailment:		
Diagnosis: J30.1 J30.81 J30.89								
1 05/15/2018	95117	1, 2, 3	1.00	AARP02 / MCAR01	MER / Y	30.00	7.44	22.56
				Totals for Claim #: C850088H		30.00	7.44	22.56
				Totals for Plan: AARP02		30.00	7.44	22.56

AETNA - ATNA9 — Claim Format: INTERGY5

Date of Service	Proc Code	Diag Xref	Units	Current / Other	Provider / As	Amount	Receipts	Net
C84009QF				Current Coverage: Tertiary		Ailment:		
Diagnosis: J45.40 J30.1 J30.81 K21.0								
1 04/17/2018	99214	1, 2, 3, 4	1.00	ATNA9 / MCAR01	KMB / Y	215.00	99.60	115.40
2 04/17/2018	94375	1	1.00	ATNA9 / MCAR01	KMB / Y	80.00	36.86	43.14
3 04/17/2018	94761	1	1.00	ATNA9 / MCAR01	KMB / Y	10.00	0.00	10.00
				Totals for Claim #: C84009QF		305.00	136.46	168.54
				Totals for Plan: ATNA9		305.00	136.46	168.54

Aetna/Banner Health Network - AETN11 — Claim Format: INTERGY5

Date of Service	Proc Code	Diag Xref	Units	Current / Other	Provider / As	Amount	Receipts	Net
C86003G6				Current Coverage: Primary		Ailment:		
Diagnosis: J30.81 J30.1 Z23								
1 05/25/2018	99214	1, 2	1.00	AETN11 /	ELC / Y	215.00	0.00	215.00
2 05/25/2018	90732	3	1.00	AETN11 /	ELC / Y	200.00	0.00	200.00
3 05/25/2018	90471	3	1.00	AETN11 /	ELC / Y	55.00	0.00	55.00
				Totals for Claim #: C86003G6		470.00	0.00	470.00
C86003G7				Current Coverage: Primary		Ailment: Quick Ailment		
Diagnosis: J30.1 J30.81								
1 05/24/2018	95117	1, 2	1.00	AETN11 /	KMB / Y	30.00	0.00	30.00
				Totals for Claim #: C86003G7		30.00	0.00	30.00
				Totals for Plan: AETN11		500.00	0.00	500.00

Figure 22

The Powerful Lure of PHI, PII, and IP

Cybercriminals Leverage PHI for Identity Theft and Other Forms of Fraud

Patient records from healthcare providers are a more valuable source of PII for identity thieves and other fraudsters because they typically contain greater detail than PII sources from other industries. Critical data points for identity thieves include dates of birth and US Social Security numbers, or their counterparts in other countries. Other useful data points include scans of identity documents and health insurance policy details.

Some criminals specialize in the sale of healthcare data or sell it on a large scale. For example, criminal forum username "calpernickles89" auctioned off a combination of adult US healthcare records and live access to US pediatric databases in June 2020. The actor started the auction at $800 USD, with bids increasing in increments of $200 USD and a "buy now" price of $2,000 USD (see Figure 23).

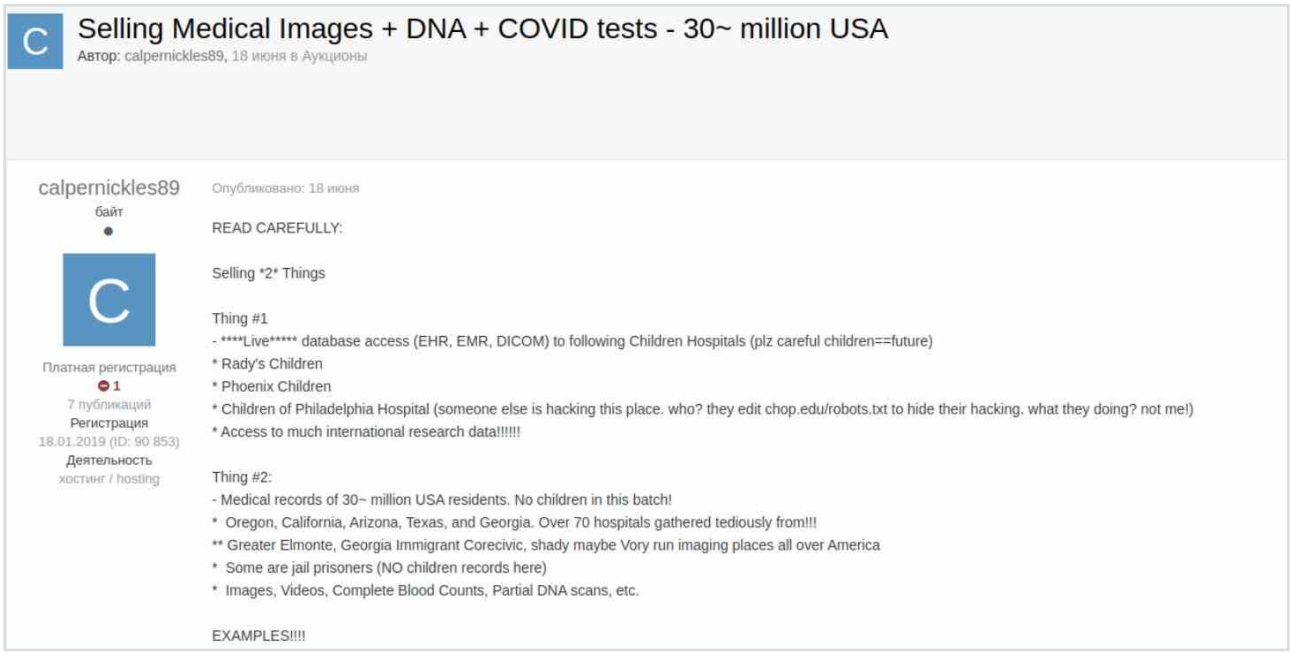


Figure 23

The adult healthcare records that were part of this auction reportedly came from over 70 hospitals in California, Arizona, Oregon, Texas, and Georgia, as well as a few prisons, and reportedly covered over 30 million individuals. The data points included DNA records, medical imagery, and COVID-19 test results. The actor also offered live access to the Electronic Health Record (EHR), Electronic Medical Record (EMR), and Digital Imaging and Communications in Medicine (DICOM) systems of three children's hospitals. Pediatric records are of greater value to identity thieves than adult healthcare records because children generally have little or no credit history and do not check their credit reports until adulthood, if ever.

The healthcare industry in the United States is the top target of these data breaches and identity theft due to its affluence and the size of its economy. Criminals do nonetheless target healthcare organizations and patient data in other countries, including developing and less affluent countries, although this data may command lower prices on the black market.

For example, in November 2020, forum username "Down3d" sold data purportedly from a breach of a mental health institution in Colombia for just $350 USD. The 23 GB of data purportedly includes SQL databases of 190,000 patients, 9,000 relatives of patients, and 7,000 employees. Other files include scans of identity documents for 16,739 employees and 23,584 patients, as well as bank account details for employees (see Figure 24).

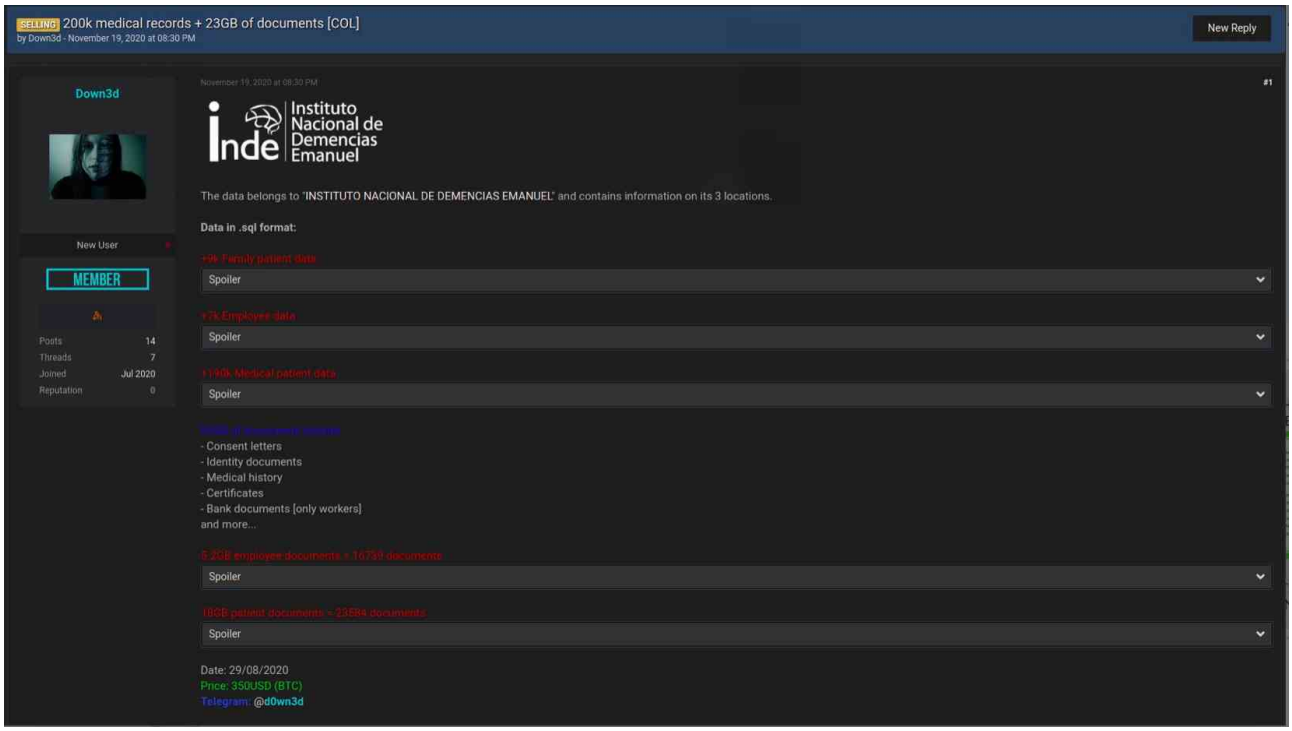


Figure 24

Here are other examples of recent patient data sales that IntSights security researchers found on underground criminal forums:

- In May 2021, username "YOMUS" offered to sell 6.8 GB worth of the medical records of 4,000 UK patients for $500 USD. The data included scans of identity documents and clinical records.
- In March 2021, username "ragnarviking" offered to sell 1 million purported patient records from an unidentified Chinese hospital system. The database included fields for names, phone numbers, genders, identity documents, street addresses, and membership IDs.
- In March 2021, username "inno36" offered to sell a database of approximately 17,500 patient records from an unidentified private hospital in the Turkish city of Ankara for $50 USD. The database included names, dates of birth, email addresses, and other PII details.
- In March 2021, username "replied" offered to sell a database of 26,600 patient records from a California-based fertility clinic. The database included fields for names, phone numbers, email addresses, passwords, and street addresses.
- In February 2021, the above-mentioned South American criminal group KelvinSecTeam offered to sell a database of patient records from the Virginia-based Lackey Clinic. The database purportedly included patient names, incomes, tax details, and health insurance details.

- In January 2021, username "Scarfac33" offered to sell a database of 700,000 patient records from Swiss Hospital in Monterrey, Mexico. The database had fields for patient names, dates of birth, addresses, and identity document numbers.
- In October 2020, username "ItsZmeyy90" shared a database of 37,000 patient records from a network of Bulgarian gynecology clinics. The database purportedly included email addresses, passwords, phone numbers, and street addresses.
- In October 2020, username "donthackme" shared a database of 65,500 patient records from a hospital in Bobruisk, Belarus. The database included names, dates of birth, and street addresses.
- In September 2020, username "Celebrate" offered to sell a database of more than 5,000 US patient records. The database included names, dates of birth, Social Security numbers, health insurance policy numbers, phone numbers, email addresses, and employment details.
- In September 2020, the aforementioned username Down3d offered to sell a database of more than 1,200 Colombian patient records. The database included names, street addresses, phone numbers, identity document numbers, and scans of identity documents.

Healthcare providers such as hospitals and doctors' offices are the primary sources of compromised PII in this industry, but they are not the only ones. Retail pharmacies also have customer data that criminals can use for fraud, further attacks, and other malicious purposes. For example, in April 2021, the aforementioned South American criminal group KelvinSecTeam offered to sell 7,000 customer records purportedly from the Salcobrand retail pharmacies in Chile. The data included names, dates of birth, genders, Chilean tax ID numbers, and email addresses for approximately 700,000 customers (see Figure 25).

Figure 25

Medical equipment providers that deal directly with patients can also yield similar PII. For example, in March 2021, Conti ransomware operators disclosed samples of patient data that they claimed to have obtained from a breach of Health Aid of Ohio. That company provides home medical equipment, such as wheelchairs, rehab mobility, home accessibility, and respiratory equipment. Similarly, in November 2020, forum username "andyleung0927" shared a database of 1,345 users of the website of Brojaw, a Taiwan-based vendor of home and personal respiratory,

breathing, and sleeping medical devices. The database included fields for customers' names, usernames, passwords, identity documents, dates of birth, street addresses, and phone numbers (see Figure 26).

Figure 26

Security researchers and healthcare security professionals have tended to focus on patients as the primary targets of PII theft in the healthcare industry. Coverage of underground criminal forums indicates that this focus on patient data is well founded, but doctors, healthcare workers, and other employees of healthcare organizations can become targets of PII theft as well. Just as in many other industries, both customers and employees can become victims of PII theft in the event of an enterprise-wide breach.

For example, in February 2021, underground criminal forum username "cesarbsfilho" (whose name suggests Brazilian or Portuguese origins, despite his use of an English-speaking forum) offered to sell access to a Mongo database from a Brazilian hospital. The database included records for 198,926 patients and 4,646 employees. The employee records included their names, dates of birth, Brazilian taxpayer numbers, Brazilian identity document numbers, and job descriptions (see Figure 27).

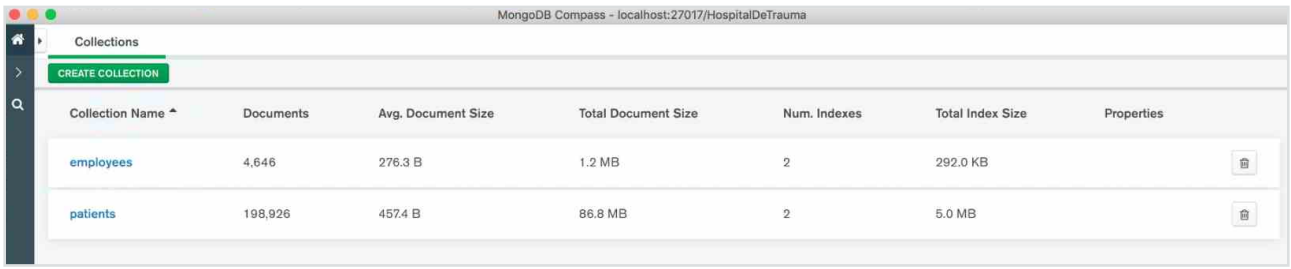


Figure 27

In April 2021, KelvinSecTeam offered to sell for $500 USD a database of approximately 200,000 US doctors. The fields for this database included names, street addresses, email addresses, phone numbers, specialties, and medical license numbers (see Figure 28). In May 2021, the same group later offered to sell a Portuguese medical database with approximately 94,000 records. The fields in this database for specialties and license numbers suggest that it was also a database of physicians or other healthcare workers (see Figure 29).

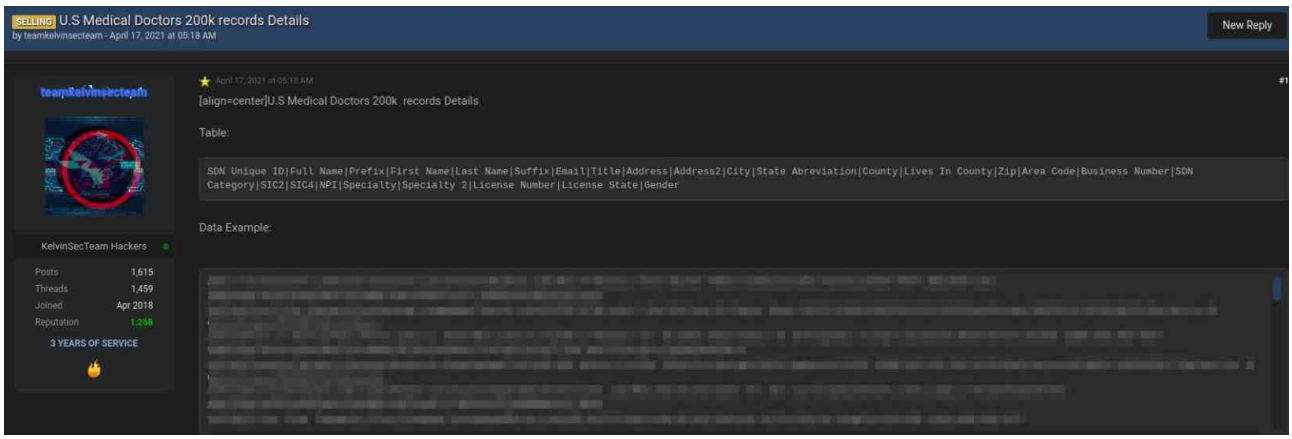


Figure 28

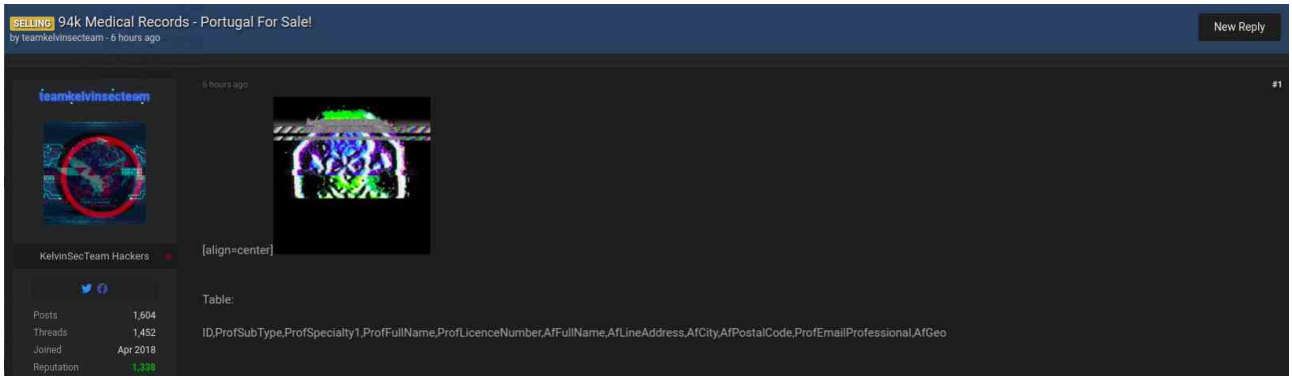


Figure 29

In November 2020, criminal forum username "husseinb" shared a purportedly compromised database of 247,000 users of PlexusMD, a professional social network for doctors and other healthcare professionals in India. The purported database included names, dates of birth, street addresses, usernames, email addresses, passwords, phone numbers, and photos for users (see Figure 30).

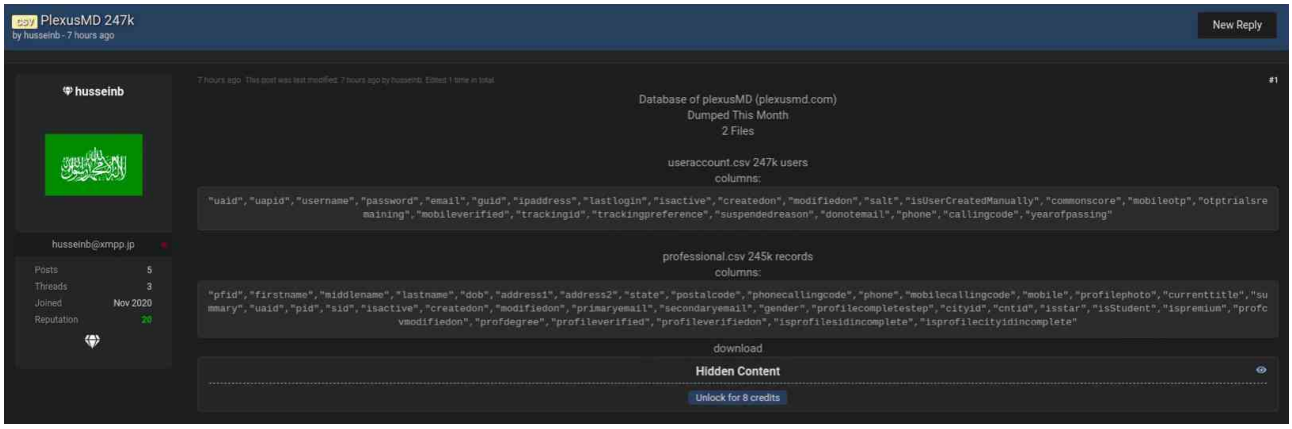


Figure 30

Even datasets like employee directories can be useful to attackers for reconnaissance purposes and in the planning and execution of social engineering or phishing attacks, both inside and outside this industry, in order to gain further access. For example, in April 2021, underground criminal forum username "ForumRAID" offered to sell the employee directory of a Chinese pharmaceutical company. The database fields for the approximately 7,000 employees included names, phone numbers, fax numbers, and email addresses (see Figure 31).

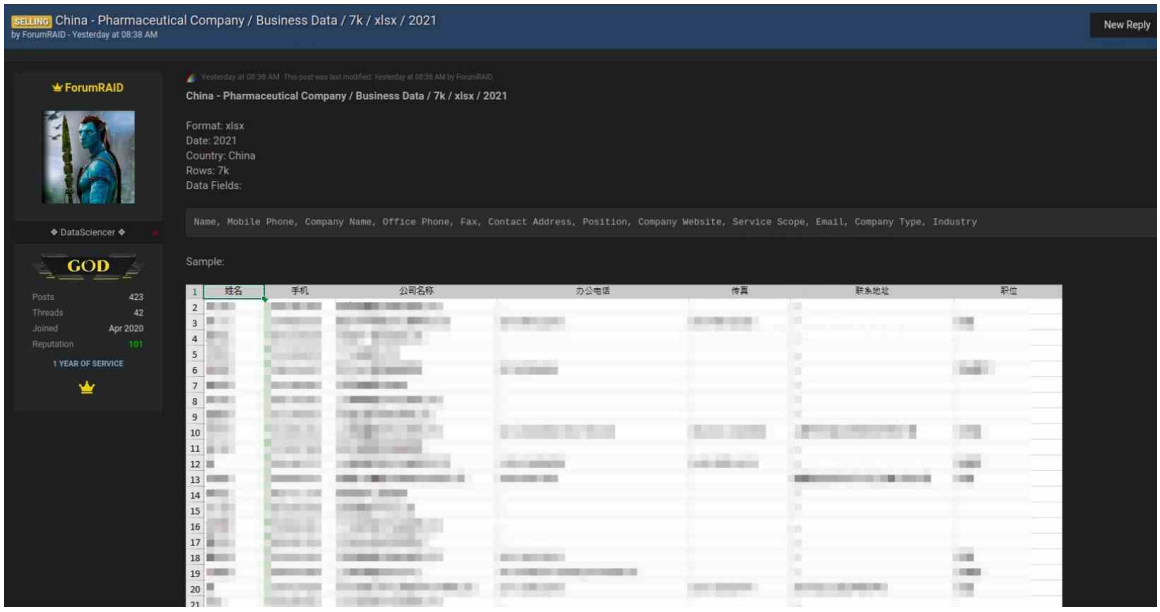


Figure 31

The collection of PII for the purpose of identity theft, such as fraudulent credit card applications, is the primary fraudulent purpose of healthcare data breaches, but it is not the only one. Health insurance details are also useful for the purposes of insurance fraud. For example, in February 2021, username "rytsoft" offered to sell Medicare details. He claimed that he had information for more than 10,000 US Medicare beneficiaries and collected details for more than 100 new victims every day. The data purportedly included beneficiaries' names, dates of birth, contact information, and Medicare coverage details (see Figure 32).

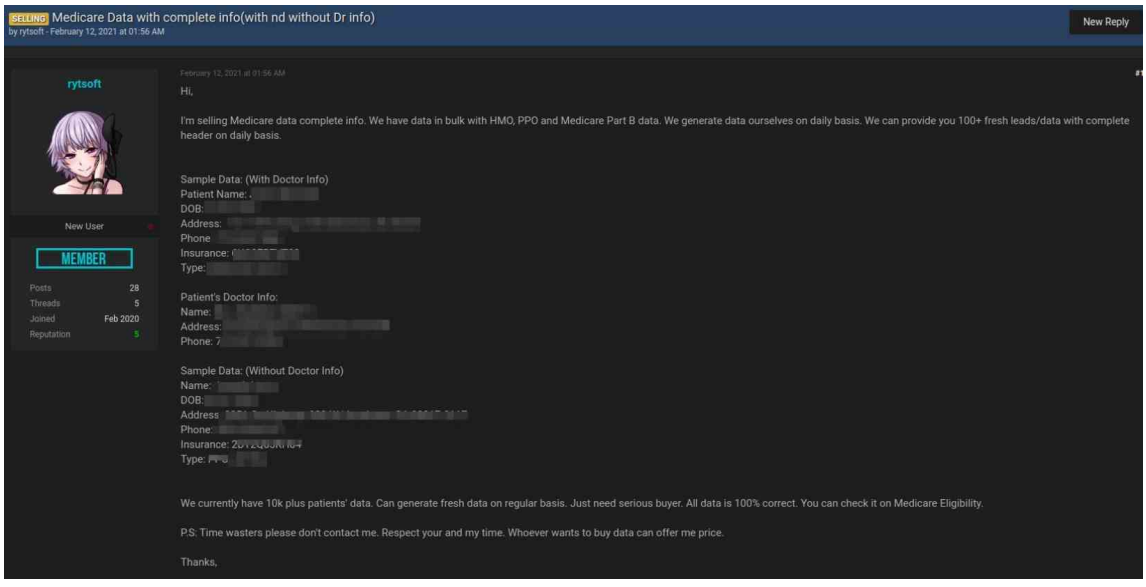


Figure 32

In November 2020, the above-mentioned username "Celebrate" offered to sell 33 SQL databases, including health insurance and billing details, from US healthcare organizations for $1,000 USD (see Figure 33). Compromised third-party vendors providing services related to health insurance are another potential source of insurance data. For example, in November 2020, operators of REvil/Sodinokibi ransomware disclosed 600 GB of data that they claimed to have obtained from a breach of Florida-based Beacon Health Solutions, which provides integrated health benefits and claims administration services. The files included claims documentation (see Figure 34).

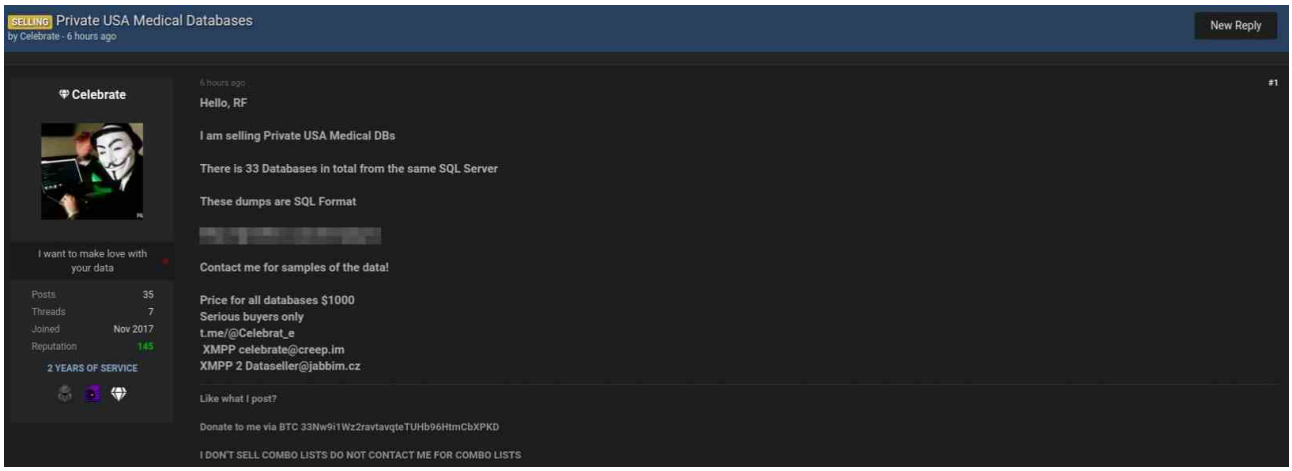


Figure 33

Figure 34

State-Sponsored Threat Actors Use PHI for Intelligence Purposes

Cybercriminals are the most well-documented consumers of PII from healthcare sources, but they are not the only ones. The greater amount of detail that PHI typically contains makes it valuable to the intelligence services of foreign governments, more so than sources of PII from other industries.

Foreign intelligence services collect PII and ingest it into searchable databases against which they conduct targeted queries in support of human intelligence (HUMINT) operations or signals intelligence (SIGINT) collection. The SIGINT components of foreign intelligence services and communities can collect information from phone numbers and email addresses within PII data sets for more coverage of select persons of interest. Overseas HUMINT operations, with intelligence officers deployed in foreign countries in search of human sources to develop and recruit, often entail queries for more information on persons of interest that they encounter, or as a source of leads for them to pursue for development or recruitment.

Other use cases for compromised PII in foreign intelligence services include the vetting of visa applicants, airline passengers, and other travelers for counterterrorism, counternarcotics, or other national security purposes. Identifiers such as dates of birth, Social Security numbers, and identity document numbers often facilitate these queries by enabling analysts to distinguish multiple individuals with the same or similar names, which can be harder if those names are in a foreign language.

Why the Anthem Breach Can't Be Forgotten

The 2014-2015 breach of US health insurance provider Anthem remains the most well-documented case of foreign governments consuming PII from healthcare sources in support of foreign HUMINT operations. The Anthem breach was also the single-largest incident to have ever affected the healthcare industry, in the United States or anywhere else in the world.

Security researchers attributed the Anthem breach, which affected 78.8 million American customers of Anthem's various brands, to the state-sponsored Chinese cyber espionage group "Deep Panda." The Anthem attackers' infrastructure had connections to infrastructure spoofing the US Office of Personnel Management (OPM), which handles security clearances for federal employees and contractors with access to classified information. OPM had also experienced a data breach attributable to Chinese cyber espionage in 2014. Security researchers posited that Chinese intelligence consumers aimed to combine and cross-reference Anthem and OPM data in order to identify US security clearance holders with significant healthcare debts, whom they believed might be vulnerable to development and recruitment as financially motivated HUMINT sources for Chinese intelligence services. HUMINT field officers seek out prospective sources that have both: a) access to non-public information that intelligence consumers seek; and b) personal vulnerabilities that HUMINT officers can exploit in order to persuade them to commit espionage on behalf of a foreign government. The OPM breach would have given them access to information on US security clearance holders. Financial vulnerabilities, such as debts, are a primary reason for HUMINT sources to commit espionage, and high healthcare costs are a leading source of indebtedness among Americans. Blue Cross Blue Shield, one of Anthem's brands, provided healthcare coverage for approximately half of the US federal workforce at the time of the incident. A precisely crafted query could thus identify US security clearance holders with large healthcare debts that might have financial reasons to become HUMINT sources for a Chinese intelligence service.

The Anthem breach was not the first reported instance of Chinese state-sponsored actors targeting the healthcare industry for PHI/PII, and it will probably not be the last. It had already emerged in 2014 that the Chinese cyber espionage group APT18 had targeted Community Health Systems (CHS), one of the largest hospital systems in the US, and collected PII data points, such as Social Security numbers, for 4.5 million patients. More recently, US national security officials publicly warned in January 2021 that China seeks to collect DNA samples from US citizens for unspecified but most likely malicious purposes. US authorities raised concerns that Chinese offers to provide COVID-19 testing capabilities in the United States aimed to enable and provide a pretext for the collection of US DNA samples. Possible applications for this data would include: surveillance, as with China's own domestic DNA database and its suppression of the Uighur ethnic minority in Xinjiang Province; manipulation, blackmail, or coercion of US citizens with health problems identifiable from DNA samples into serving as HUMINT sources for Chinese intelligence services; and bioengineering or biotechnology research for economic gain or geopolitical advantage. US DNA may be of greater research value than that of many other countries due to the greater ethnic and genetic diversity of the US population. US intelligence officials claim that China has already conducted human tests in the hopes of producing genetically enhanced "super soldiers." As of this writing, there is no evidence of Chinese actors conducting cyberattacks to collect US DNA data, but the purported use of COVID-19 testing as an opportunity to collect such data nonetheless indicates a willingness to use covert methods to obtain it.

Healthcare, Pharmaceutical, and Biotechnology Companies Have Valuable IP

Healthcare, pharmaceuticals, and biotechnology are key target areas for China's ambitious economic development plans. The theft of foreign intellectual property by state-sponsored Chinese cyber espionage groups is a key way for China to enhance its competitiveness against foreign businesses in key economic fields, including this industry. Stealing foreign intellectual property reduces or eliminates R&D costs and enables Chinese businesses to produce cost-competitive copies of foreign products at a fraction of their competitors' prices, thus capturing market share from them. Multiple Chinese cyber espionage groups have targeted healthcare organizations and pharmaceutical and biotechnology companies in order to collect their intellectual property. Below are examples of Chinese cyber espionage groups with a previous track record of targeting this industry.

- APT9 has targeted primarily pharmaceutical and biotechnology companies, among others. APT9, also known as Nightshade Panda, reportedly leveraged a trusted technology relationship between two biotechnology companies to expand its initial access from one of those two companies to the other one.
- APT10 has targeted businesses in many different industries, including pharmaceuticals and biotechnology. The long-standing APT10, also known as Cloud Hopper, Stone Panda, and Red Apollo, was a pioneer of the use of technology supply chain attacks, via compromises of managed service providers (MSPs), to efficiently infect large numbers of victims.
- APT 22 has focused on the targeting of healthcare, pharmaceutical, and biomedical research around the world. APT22, also known as Barista, uses strategic web compromises, or watering hole attacks, to infect victims. It also gains access to enterprise networks via web shells that it installs on vulnerable, public-facing web servers.
- APT41 has targeted a wide range of businesses, including pharmaceutical companies and medical device manufacturers. Its techniques have included the use of stolen code signing certificates in its malware payloads to evade detection and the injection of malicious code into legitimate production environments as a software supply chain attack.

State-sponsored Iranian cyber espionage groups have also targeted foreign intellectual property in the healthcare and pharmaceutical industry, but for different economic reasons. One of the top goals of Iranian cyber espionage against foreign businesses has been the circumvention of international sanctions against Iran for its nuclear program. These sanctions make it difficult or impossible for Iran to import many foreign products. Iran's solution to this problem has been to steal foreign intellectual property with which to produce domestic copies of those foreign products, in a form of import substitution. International sanctions against Iran have exceptions for healthcare and other humanitarian products, but many foreign banks and businesses are still wary of engaging in such transactions with Iran out of a spirit of "overcompliance." Foreign healthcare and pharmaceutical research has thus become a target of Iranian cyber espionage. For example, the state-sponsored **Mabna Institute**, also known as "Silent Librarian," has targeted Western healthcare organizations, among others in many different fields, in order to gain access to Western research, including medical journals. The Mabna Institute specializes in phishing and brute force attacks on credentials in order to gain access. Notable healthcare targets of the Mabna Institute have included the Memorial Sloan Kettering Cancer Center and Ohio State Wexner Medical Center.

Other state-sponsored Iranian cyber espionage actors further targeted US and Israeli medical researchers in the fields of genetics, oncology, and neurology in the December 2020 "BadBlood" phishing campaign. It is unclear why the Iranian actors had such a specific interest in those particular medical fields, beyond the Mabna Institute's previous targeting of a US cancer center. It is also unclear why they chose to focus on those particular medical fields in the midst of the COVID-19 pandemic, which involves a respiratory virus and has had a severe impact on Iran. The US is an obvious target, both for its large number of medical researchers and its long-standing adversarial relationship with Iran. For decades, Iran has had a similarly adversarial relationship with Israel, which has thus been a top target of Iranian cyber espionage as well. It is nonetheless unclear why this campaign would demonstrate such a specific interest in the medical research community of such a small country when there are more researchers and perhaps more research to steal in other countries.

Criminals also seek access to the high-value intellectual property of pharmaceutical companies, albeit for personal financial gain, rather than national-level economic purposes. For example, in July 2021, IntSights researchers discovered this sale of purportedly compromised data from two Israeli pharmaceutical companies by username "zerox296." The 500GB of data on sale for $300,000 USD reportedly included product details and experimental data, as well as employee information, contracts, and invoices (see Figure 35).

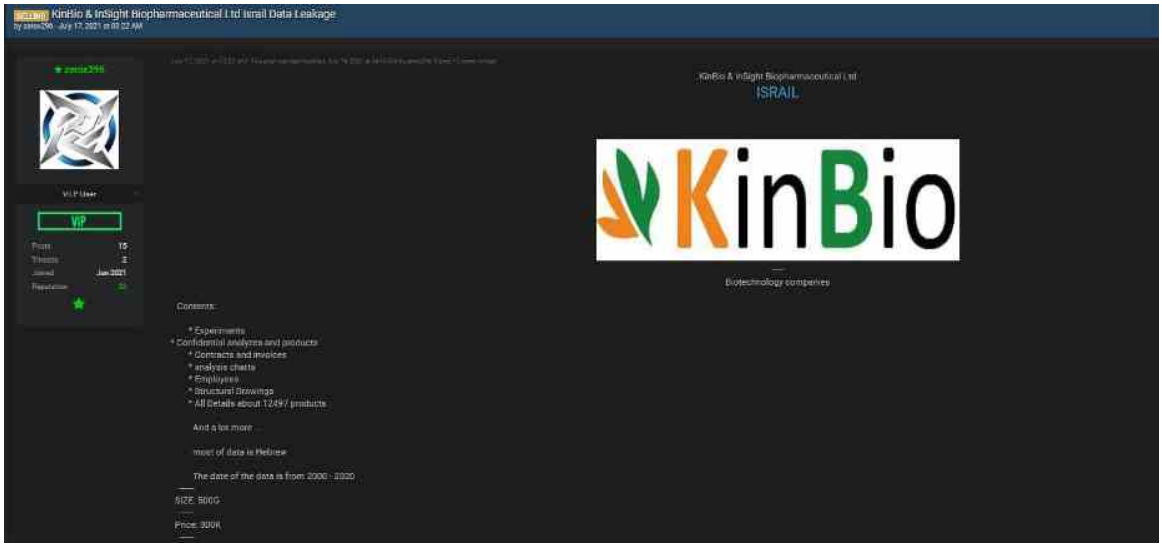


Figure 35

The intellectual property of pharmaceutical companies is also vulnerable to exposure via the data disclosure extortion component of many ransomware attacks. Indeed, a ransomware deployment may be merely the final stage of a much longer and wider breach aiming to collect profitable information and achieve other malicious objectives before seeking to extract one final form of revenue from a victim in the form of a ransom payment. For example, in August 2020, operators of the Dopple Paymer ransomware family disclosed data that they claimed to have obtained from a breach of the US pharmaceutical company Amphastar, which specializes in injectable and inhaled products. The data included several files of insulin research, as well as business documentation, such as files on company stocks, audits, and confidentiality agreements (see Figure 36).

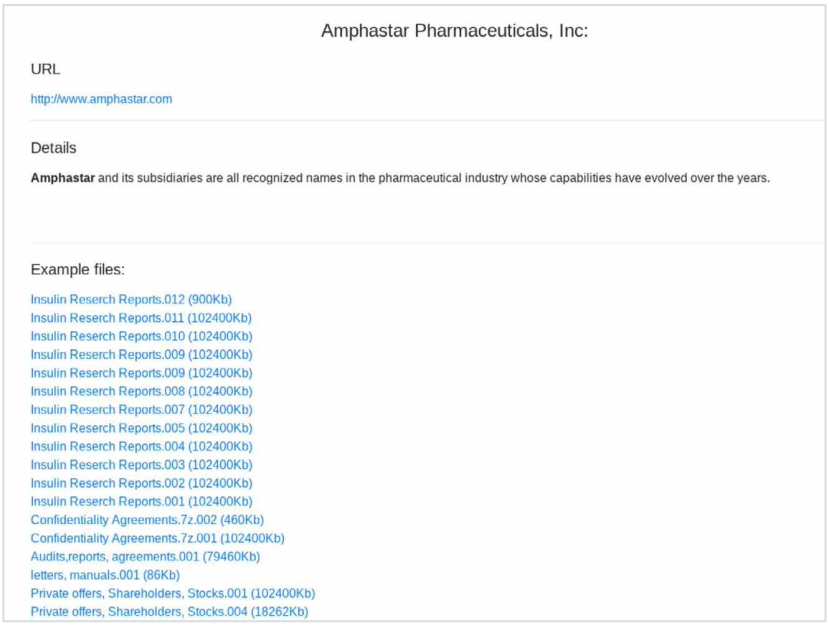


Figure 36

Similarly, in May 2021, "CL0P" ransomware operators published a sample of data that they claimed to have obtained from a breach of Aurobindo Pharma, an Indian pharmaceutical manufacturer. The sample included scans of employee identity documents and pharmaceutical product details (see Figure 37).

Figure 37

Pharmaceutical companies may be the most valuable source of intellectual property in this industry, but medical device manufacturers and other manufacturers in this industry also have intellectual property for their products to protect as well. For example, in May 2021, "N3TW0RM" ransomware operators threatened to disclose 1.1 TB of data that they claimed to have obtained from a breach of Israeli medical device manufacturer Eitan Medical. The ransomware operators posted a directory of project source code repositories that they threatened to leak, several of which contained the word "pump" (see Figure 38).

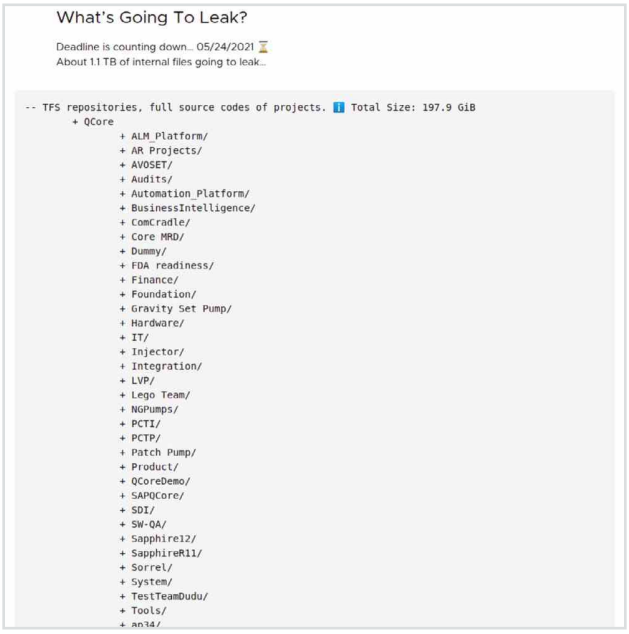


Figure 38

Producers of diagnostic lab tests also have intellectual property that ransomware operators can disclose in extortion attempts. For example, in January 2021, operators of Babuk ransomware posted a sample of intellectual property that they claimed to have obtained from a breach of Germany-based Human Diagnostics, which produces laboratory tests for human samples. The Babuk actors threatened to publish the whole 100 GB of data if the victim failed to pay the ransom within six business days (see Figure 39).

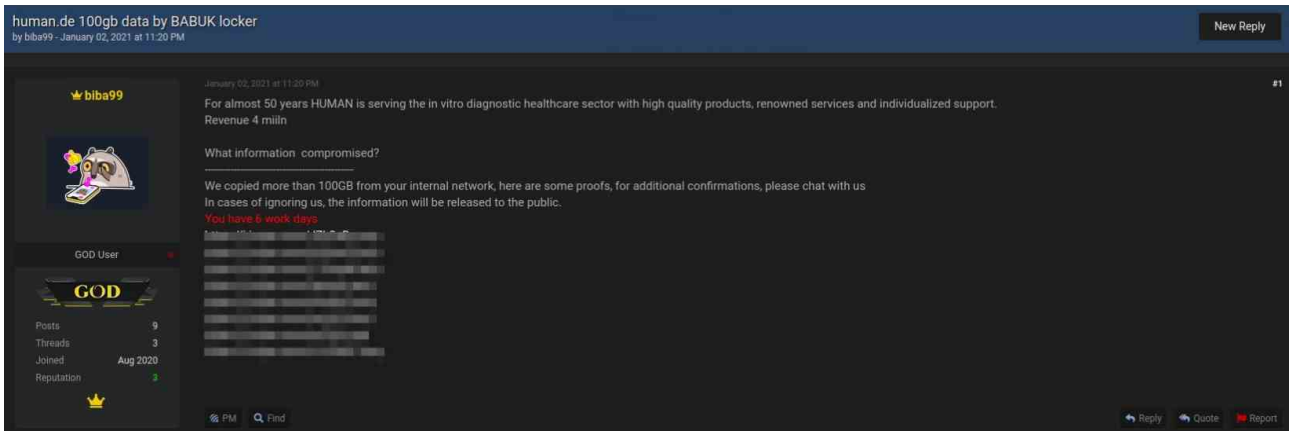


Figure 39

Industry Recommendations

Healthcare and pharmaceutical organizations can take several steps to improve their risk profiles and security postures. This section outlines the steps that can make the greatest impact.

Establish Priorities

To address the most critical vulnerabilities first, as well as to avoid overwhelm, prioritization is key. Healthcare and pharmaceutical organizations should prioritize the top threats to their respective businesses and then identify which of their assets are most likely to come under attack or to enable a compromise.

- A prioritized asset inventory, which ranks devices and data sets according to their respective levels of risk, can help organizations allocate resources to wherever the need is greatest.
- Certain devices and data sets in this industry are clearly of greater interest to attackers and should thus receive extra protection. These assets include: medical devices, which are common entry points or persistence mechanisms for network intrusions; patient data, which criminals can use for fraud and ransomware extortion and foreign governments can use for intelligence operations; intellectual property, which criminals can sell and foreign governments can use for their national economic goals; and non-clinical business records that criminals can use for fraud, such as HR and payroll records, employees' PII, accounting and tax records, etc.
- Additional layers of defense for these key assets can include network segmentation for sensitive devices or servers storing key data sets, the encryption of files containing these key data sets, and heightened levels of scrutiny and security hygiene for medical devices.
- Establishing Priority Intelligence Requirements (PIR) helps determine the scope of an organization's cyber threat intelligence needs and set priorities, based on its specific risk profiles. Healthcare organizations should prioritize the collection of cyber threat intelligence on both ransomware attacks and the theft of patient records, which are top threats to such organizations. In contrast, a pharmaceutical company should prioritize the collection of intelligence on intellectual property theft.
- A prioritized asset inventory can complement and help to refine a PIR list, as organizations can tailor their PIRs based on an assessment of which attackers are most likely to target their organizations to gain access to their most valuable assets.

Integrate Cyber Threat Intelligence

Cyber threat intelligence is a critical line of defense. It enables organizations to learn about threats before they affect them and to seize that window of opportunity to improve and tailor their defenses against those attacks if and when they eventually do affect them.

Organizations should strive to strike the right balance in their respective coverage of both criminal and state-sponsored threats. In the case of the healthcare and pharmaceutical industry, criminal attacks are clearly more common and should be given higher priority; however, these organizations should not disregard state-sponsored threats.

Private sector organizations with no direct geopolitical, military, or national security nexus may mistakenly conclude that they are not targets of interest to state-sponsored threat actors because of their political neutrality. Healthcare

and pharmaceutical organizations possess data that foreign governments can use for a variety of purposes, and many of the most prolific and sophisticated sponsors of cyberattacks, such as Russia, China, Iran, and North Korea, are willing to attack politically neutral organizations in order to obtain that data. The COVID-19 pandemic has increased the risk of state-sponsored attacks for certain organizations in this industry, particularly pharmaceutical companies, as governments urgently seek solutions to this global public health crisis.

Robust threat intelligence coverage should come from a variety of sources. A great deal of threat intelligence comes from purely technical sources, such as customer telemetry from the anti-virus software or the detection and response platforms of various security vendors. These feeds are valuable, but it is important to supplement these technical sources with human sources, such as the underground criminal forums from which we have drawn so many examples in this report. At the end of the day, human actors rather than technology are the ultimate sources of cyberattacks. Technology merely gives attackers the means with which to achieve their goals.

It is thus critical to understand the human actors responsible for these threats, including:

- Their plans and intentions
- The tactics, techniques, and procedures (TTPs) that they use
- The data sets and types of access they seek
- The ways in which they monetize or consume compromised data

Build a Robust Ransomware Defense

Ransomware is a top threat to this industry, as evidenced by the sheer amount of data presented in this report. What makes ransomware unique is the coercive element of extortion.

The best defense against ransomware is to eliminate the temptation to pay ransom with offline backups and strong encryption. A robust backup strategy should include:

- Frequent backups, to minimize the amount of data loss in the event of a restoration
- Segmented backups, to prevent attackers from moving laterally and encrypting or deleting backups
- Redundant backups, to account for the possibility that attackers will encrypt or delete at least one set of backups

Ransomware operators have learned that backups are a strong defense against ransomware and have added the threat of data disclosure in order to circumvent that defense. The best defense against the threat of data disclosure (other than preventing the compromise in the first place) is to encrypt the most sensitive files, the disclosure of which would cause the greatest harm to the organization. Ransomware operators often choose the files that they disclose, or threaten to disclose, based on the perceived greater coercive impact of disclosing the most sensitive data sets, such as patient data or intellectual property.

Balance Usability and Cybersecurity

It is critical for healthcare organizations to strike the right balance between usability and security. Finding the best ways to improve security posture with minimal impact on usability can help an organization in the long run.

For example, implementing multi-factor authentication (MFA) via mobile authenticator apps, rather than SMS, is better both from a security perspective and from a usability perspective. SMS-based MFA codes are vulnerable to

interception via SIM swapping attacks. SMS-based MFA is also disadvantageous from a usability perspective due to its dependence on mobile service providers, which may cause delays or disruptions in the receipt of MFA codes via SMS. MFA codes from mobile authenticator apps are not vulnerable to SIM swapping attacks, delays, or disruptions in mobile service. Some MFA apps offer users another way to improve convenience by enabling them to authenticate via a "push" that users can accept on their devices with one touch, rather than taking the time to manually enter MFA codes.

There are other ways to improve an organization's security posture that have little or no impact on usability. For example, disabling RDP services that no one is using should not have any impact on users but can yield significant security benefits, given the popularity of RDP as a target for brute force attacks and as an access vector for ransomware operators in particular.

Similarly, as many employees return to physical workplaces, security teams should disable VPN credentials or other remote access services that formerly remote employees no longer need. Leaving remote access services that are no longer in use does not improve usability but does increase security risks unnecessarily by expanding the available attack surface for attackers to exploit. It is already a well-established best practice to limit privileges to the bare minimum that users need in order to do their jobs; by the same token, organizations should limit the various forms of remote access to the bare minimum that users need in order to perform their duties.

Conclusion

The healthcare and pharmaceutical industry is encountering an unprecedented era. At a single point in time, the industry is challenged with advanced threats that are exploiting technology shortcomings, staff overwhelm, and a booming underground business community. Yet, while the situation may appear desperate, it can be overcome. Building immunity against today's threats requires keeping a finger on the pulse of the cyber threat landscape, and then building and executing on a plan that strengthens the organization's security posture over time.

Healthcare and pharmaceutical organizations that effectively prioritize and use all tools available to them, including the necessary technologies and supplemental external expertise, will be better positioned to succeed in both the current and future cyber threat landscape.

About IntSights

IntSights, **a Rapid7 company**, enables organizations of any type or size to gain the full benefits of external threat intelligence, no matter the size or sophistication of their threat intelligence programs. Unlike any other solution on the market, IntSights takes the complexity out of threat intelligence and delivers instant value without the heavy lift or sizable resource allocation that traditional threat intelligence solutions require. Designed to scale, IntSights is for any company, and frictionless integration of our real-time cyber threat intelligence with existing security infrastructure allows enterprises to maximize return on investment.

IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit **intsights.com** or connect with us on **LinkedIn**, **Twitter**, and **Facebook**.