REPORT

McAfee
Together is power.

Health Warning

Cyberattacks are targeting the health care industry

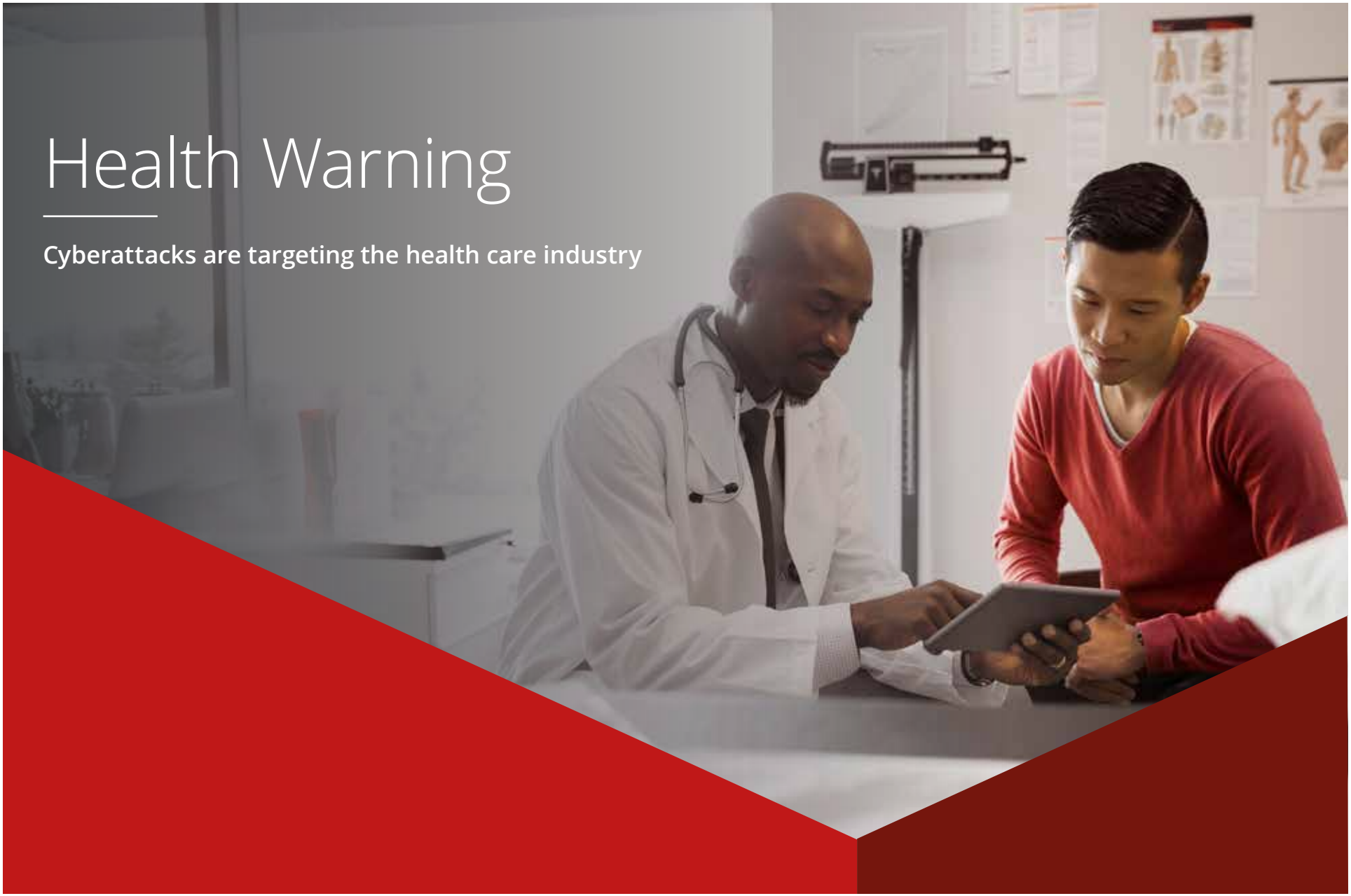


Table of Contents

Authors

This report was researched and written by:

Advanced Programs Group

- Christiaan Beek
- Charles McFarland
- Raj Samani

Executive Summary

We have all read about the nonperishable nature of medical data. Whether our medical histories or intellectual property for the next wonder drug, when the bad guys have that data, it is not easy to recover. Why is medical data being stolen? Is it a target or simply collateral damage as part of a different attack? If it is targeted, then that suggests a clear demand; and if there is a demand, then there must be a return on investment. What is the big picture?

This research report is about theft in the health care industry. Specifically, we will describe the marketplace for stolen health care industry data and examine the motivations for its theft.

In the McAfee® Labs research report ***The Hidden Data Economy***, we examined data breaches involving the theft of financial data, particularly payment card information. In that report, we did not find medical data for sale. We knew that medical data was being stolen, but had not seen it in "dark markets." After further investigation, we can now lay out what we have found.

—Raj Samani, CTO of McAfee for Europe, the Middle East, and Africa

@Raj_Samani
@McAfee_Labs

Hidden in Plain Sight

We learned from ***The Hidden Data Economy*** report that a marketplace for stolen data exists, and that business is very good. Indeed, the growing stream of compromised organizations and stolen data has led to such a dramatic decrease in the prices of such data that we have to wonder when it will strike bottom. In fact, the volume of payment card data has led to some fascinating business models as sellers attempt to attract buyers.

Our research surprised us in that medical data was ominously absent from the treasure trove of stolen data for sale. We did not specifically look for such data for sale, but we expected to find it because we know it is being stolen. The absence of medical data for sale led us to this research report.

Rather than simply providing screenshots of stolen personal medical data for sale (assuming we could find them), we have dug deeper to understand which other parties within the health care industry are being compromised. For example, are pharmaceutical companies being attacked?

In February, we posted the blog "**Ransomware Targets Health Care Sector**," which discussed a ransomware incident against a US hospital. The blog states that ransomware is now targeting organizations—as opposed to the scattergun approach of the past—and that the health care industry is now a target for cybercriminals.

Thus while this report examines stolen medical data for sale, other types of attacks are being perpetrated against health care organizations.

Before we dive into the findings, we must make one thing clear: It is not our intention to stir up fear. Rather, our aim is to document the threat landscape so that health care organizations can take action. For the health care sector, this is imperative because we cannot simply change medical records as we can when payment cards are stolen. Indeed, the nonperishable nature of medical records makes them particularly valuable. Because the ability to reduce the impact of a medical data breach is significantly diminished, we must do all we can to reduce the likelihood of successful attacks. The first step in this process is to understand the threat.

Medical Data for Sale?

The first issue to examine is whether stolen medical data is being offered for sale. Our initial assumption was that we were simply not looking in the right places in our prior research. This assumption has proven to be accurate. Quickly, we discovered dark web vendors offering for sale huge data dumps of stolen medical data. In some instances, its availability was highly publicized. In Figure 1, one seller offered for sale a database containing the personal medical data of 397,000 patients. What is included within this data dump is detailed by the seller in Figure 2.

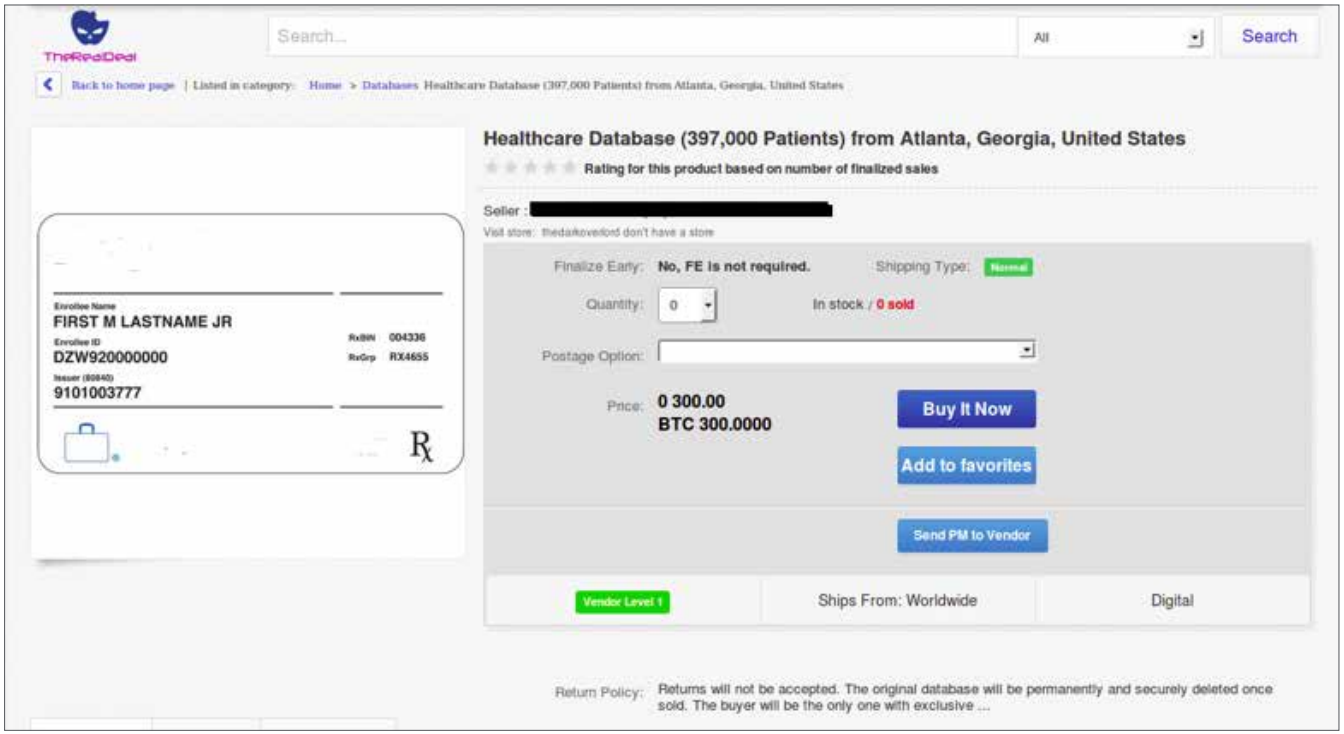


Figure 1. A health care database for sale.

Figure 2. Data fields from a health care dump.

In the preceding example, not only are the names and addresses of patients included, but also data about their health care insurance providers, both primary and secondary, as well as other data that may be of value to would-be buyers. The cost of such records is remarkable; compared with other data dumps, the price for medical data is considerably higher. We offer details later in this report.

There is no shortage of data dumps to examine. Figure 3 contains an offer to sell personal medical data stolen from a health care organization located in Farmington, Missouri. This offer is from the same seller as quoted in Figures 1 and 2.

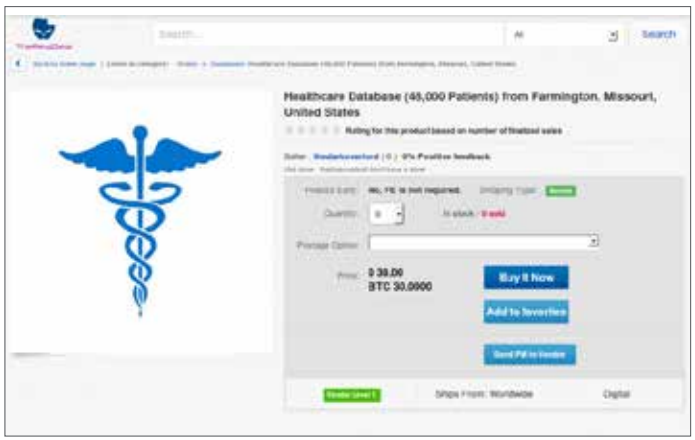


Figure 3. Details from a second breach.

This seller does not stop there, offering a third database of personal medical records stolen from another compromised health care organization, as depicted in Figure 4.

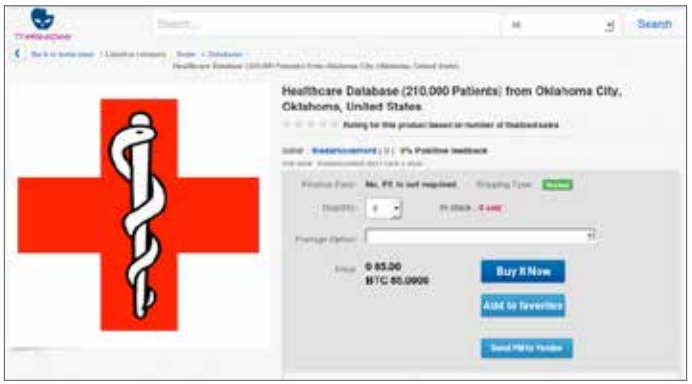


Figure 4. Details from a third breach.

You may wonder why we state that the seller actually stole the data. We found that the seller provided evidence of access to the breached organizations. In an interview with Deepdotweb.com, a number of screenshots were provided, one of which is shown in Figure 5.

Figure 5. Data from a breached health care organization.

This seller appears to be exploiting a vulnerability in the remote desktop protocol to compromise these organizations.

Simply stealing medical data is only part of the story. Despite attempts by Hollywood to show that the art of hacking takes just a matter of minutes while randomly typing characters on a keyboard, the truth is rather different, taking much more time and effort. Further, cybercriminals think in terms of a return on their investment. For this seller, the ability to turn a profit to pay for the investment in time (and possibly any tools required) is likely to be the key motivator. In **an interview that this seller gave to Motherboard**, he or she was apparently well rewarded for the time spent. The seller stated "Someone wanted to buy all the [insurance company] records specifically." The seller explained that this effort has netted $100,000 thus far.

This episode suggests two things. First, stolen medical records are for sale (as we had expected) and, second, there is clearly a demand for such data. This conclusion is not based on just one seller. We did not have to go far to find more evidence.

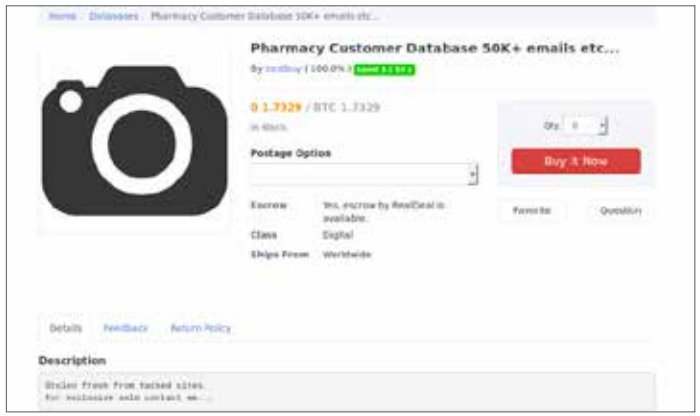


Figure 6. More data for sale.

The seller of the preceding data dump is not the same as in the earlier examples, although the offer is on the same marketplace. The seller appears to be active, with 100% positive feedback from 15 interactions to date. These positive reviews were likely gained as a seller, as the recent feedback clearly indicates.

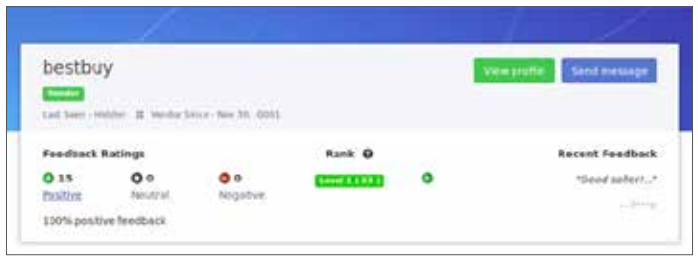


Figure 7. Good feedback for this seller.

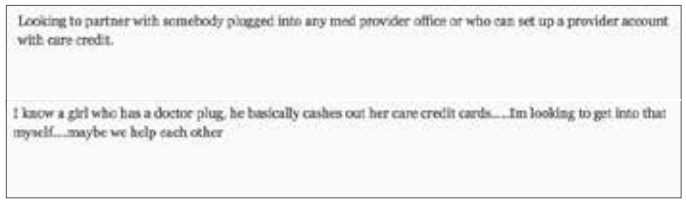
We can conclude that medical data across the health care sector is being stolen and sold. Not only is it being sold, but it is also openly advertised for sale. In certain cases, the seller even boasts of the compromise using social media.

At the time of this writing, the Twitter account for the preceding user is no longer functioning. However, there are reports that the individual(s) behind the account has resurfaced with a data dump from another compromised health care organization. Or it may be a copycat. We saw **news in mid-September** of yet another health care organization being extorted with the threat of released compromised records. This seller appears to first communicate with a breached organization threatening to release the stolen medical data unless a fee is paid.

We have seen from other sources many other examples of stolen medical data from health care organizations being offered for sale. There is clearly a marketplace for stolen medical data.

The Insider

There is evidence on certain dark web forums that criminals seek insiders within health care organizations. In the following example, we show that insiders are being sought to establish an account with Care Credit, a health care financing credit card company. This is not strictly medical data, and is more akin to the payment card fraud we discussed in our report *The Hidden Data Economy*.



Is Medical Data Worth More?

Financial data, such as payment card information, has many established markets. The going price for a single record of "fullz" information—full packages of individuals' identifying information, with names, Social Security numbers, birth dates, and account numbers—ranges between $14 to more than $25 per record. Less established sellers have low introductory prices; we have recently seen around $20 per record for small-scale purchases. Wholesale prices can be even lower, as low as $3 per card sold in bulk. Medical records, on the other hand, appear to be highly variable and range from a fraction of a cent to $2.42 per record. This price is a significantly lower than individual payment card prices but only slightly less than wholesale card prices.

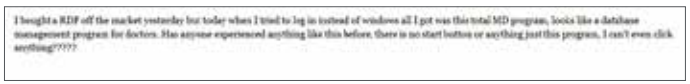
Do these prices mean medical data is not worth as much as financial data? Perhaps, but the markets are different. Some sellers have taken advantage of parallel markets to increase their profits. On the underground market forum AlphaBay, the user Oldgollum sold 40,000 medical records for $500 but specifically removed the financial data, which was sold separately. Oldgollum is essentially double-dipping to get the most from both markets. Financial data can also be sold in individual records or in bulk. Medical data appears to be sold only in bulk at this time, which reduces the per-record price to something near the wholesale prices of cards. Certainly medical data adds value to the transaction. The sellers aim to ensure they extract maximum profit from both markets and do not expect to sell at a premium to either side.

Financial data is not the only type of data we can use to compare market dynamics. Take, for example, two recent social media account dumps, both selling in bulk between 65 million and 167 million accounts, but also gaining only fractions of a penny per record. Even more recent leaks involving Bitcoin forums have similar per-record pricing. Our findings on medical data exceed this amount but do not yet sell at the rate of established markets such as payment cards. The stolen medical data still appears to be taking shape, but the current ecosystem already has a higher per-record value than in markets of nonfinancial account data. Is medical data worth more? It seems to be worth something between traditional database dumps and payment card data. If the medical data contains financial data, it appears to be more profitable to sell them separately rather than together.

Cybercrime-as-a-Service for Health Care

When McAfee Labs published the research report ***Cybercrime Exposed***, the concept of cybercrime-as-a-service was a relatively new idea. The fact that components of a cyberattack can be outsourced was not commonly known. Today this is old news, with cybercrime-as-a-service a very well publicized business model. This business model applies equally to the health care sector.

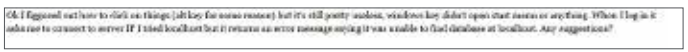
We now see cybercrime-as-a-service operating in the health care sector, with evidence that vulnerabilities are being sold and organizations are being compromised as a service. Let's take a look an online exchange that appears elementary, but this exchange discusses the theft of a large volume of personal medical data of patients who are unaware that their information has been stolen by an as-a-service criminal.


I bought a RDP off the market yesterday but today when I tried to log in instead of windows all I got was this total MD program, looks like a database management program for doctors. Has anyone experienced anything like this before, there is no start button or anything just this program, I can't even click anything????

The RDP vulnerability in the first comment is the same remote desktop protocol flaw that was exploited by our seller in the first section. The individual(s) seeking help received some guidance:


export the DB and sell it for profit obv

That is a pretty simple instruction. However, it seems the request was considerably more tactical:


Ok I figured out how to click on things (alt key for some reason) but it's still pretty useless, windows key didn't open start menu or anything. When I log in it asks me to connect to server IP. I tried localhost but it returns an error message saying it was unable to find database at localhost. Any suggestions?

The discussion continued and following some additional support interaction, the original poster was able to successfully troubleshoot the issue:


**********AMAZING UPDATE**********

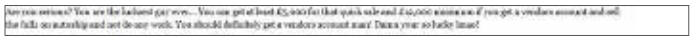
Thanks to some much needed help from [redacted] we were able to access the medical database which contains over 1000 FULLZ!!!!!!

see pic below:

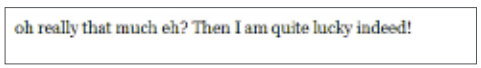
[URL]http[redacted]

Looking to sell the whole thing PM me if you're interested!

The response to this posting demonstrates something that we illustrated in the first section: the presence of market demand.


Are you serious? You are the luckiest guy ever... You can get at least £5,000 for that quick sale and £15,000 maximum if you get a vendors account and sell the fulls so mutorship and not do any work. You should definitely get a vendors account mate! Damn your so lucky lmao!

To put this in perspective, a relatively non–technically proficient cyber thief buys tools to exploit a vulnerable organization, uses them with a little free technical support, and then extracts 1,000 records that could net him £12,000 (about $15,564). If we wanted evidence that cybercrime-as-a-service is in full swing within the health care sector, this exchange makes it clear. After more congratulatory messages, the cybercriminal seemed somewhat surprised at the amount of revenue he or she could generate from the sale of the stolen medical data:


oh really that much eh? Then I am quite lucky indeed!

In this example, the process could have been even simpler. Rather than "buying the RDP," the attacker could simply have acquired an account belonging to a health care organization.

As we pointed out in *Cybercrime Exposed*, cybercriminals today require little technical knowledge, only the means to pay for help from someone with the requisite experience. In fact, there are a multitude of sellers offering stolen data to buyers who do not need to get involved with direct attacks on organizations:


Almost every week I have FRESH breaches in USA Healthcare/insurance sector.
No specific requests (like specific clinic/hospital), no pieces selling, no timewasters, ONLY BULK, ETC.

We witness countless buyers complaining that the wares they purchase from sellers never turn up. In one posting from a credible seller on a primarily Russian-speaking forum, Exploit, a seller talks about getting information from a hospital network. The topic of the thread, translated from Russian, is "RDP access to the US hospital network." The seller was peddling patient lists, providers, emails, social security numbers, dates of birth, medical records, and other information. The seller also offers various databases of information that include similar data. He has posted in forums and marketplaces such as Altenen, Lampeduza, and various carding forums since 2011 and has a history of selling personally identifiable information. Thus, there is a high degree of confidence that the medical data offered for sale is real.

With these examples, we have detailed criminal activities whose motive is financial gain, with clear routes to monetization. Of course, buyers of stolen data may have other motives, but from breach to resale of stolen data, the motivation of these attackers is clearly financial.

Although personal or sensitive data has value, it is likely that intellectual property or other types of medical-related data has higher value. We could write a full report on that topic alone, but for now we'll provide just a glimpse.

Biotech/Pharma Under the Spotlight

Holding health care organizations ransom or targeting them for theft of personal data is a relatively recent phenomenon. Targeting biotechnology and pharmaceutical firms for theft of intellectual property appears to be considerably older. Early cases go **as far back as 2008**, with reports that data sought include "drug trial information, chemical formulas, and confidential data for all drugs sold in the US market." Clearly, the economic value of such information is considerably higher than the cents-per-record market this and other reports have identified.

Opportunities like this apparently justify the cost of a cyber theft operation that "employs hundreds of people and makes use of at least 1,000 servers." Such attacks have not entirely focused on private sector firms. For example, the US Food and Drug Administration "**has been among the most targeted agencies because of its role as the starting point for bringing new products to market**." To understand the scale of the attempted intrusions, **a Freedom of Information Act request** found "1,036 incidents had been reported between 2013 and 2015. Of those, half involved illegitimate, unauthorized access into FDA computers. Another 21 percent were classified as probes or scans—similar to phishing—and 19 percent were malware intrusions."

Malware appears to be a common attack vector in attempts to compromise biotech and pharma networks, but in other cases malicious insiders **have been employed to extract data for gain**. In one case, for example, the cyber thief "**intended to use the information to launch its own competitor companies**."

We have been careful not to speculate about attribution because doing so requires an investigation that goes well beyond technical indicators. Despite third-party research making assertions on the sources of attacks based on such indicators, our intention is to demonstrate the value of such data, and that apparently resource-rich threat actors are successful in their activities.

The use of malware was discussed in **a Form 8-K submission** by Community Health Systems to the US Securities and Exchange Commission. They reported that "sophisticated malware" attacked the company's system. The submission noted that the attacker "sought valuable intellectual property, such as medical device and equipment development data." The forensic team in charge of the investigation reported "this group typically targets companies in the aerospace and defense, construction and engineering, technology, financial services, and **healthcare industry verticals**."

In most cases, spear phishing is the precursor to infection, as was demonstrated in **an attack against the National Research Council**. In this example, the attack "began with the collection of valid email addresses for research council employees," according to a study conducted by the Canadian Cyber Incident Response Centre. The attack was followed by the installation of

malware after the recipients clicked on malicious links. Despite its simplicity, spear phishing appears to be a recurring theme even when the objective is the theft of intellectual property, trade secrets, and other sensitive or proprietary information.

Our research continues into health care attacks whose aim is intellectual property theft. We can debate the motivation and the actors behind these attacks, but there is no doubt that pharmaceutical and biotech firms must remain vigilant because their most valued assets are in the spotlight of determined threat actors. As a vice president at Reliance Life Sciences **stated**, "Hackers love pharmaceutical companies as we have some high-value critical assets like [intellectual property rights], formula of various drugs. Besides, coming from a large industry house also makes us a loved target."

Conclusion

The examples of a hidden data economy for stolen medical data represents only the tip of an iceberg. We omitted many other categories and services, but we hope these examples make some threats clear. In this report, we discussed stolen health care–related data offered for sale. We showed that cybercriminals also buy products that enable attacks. This includes the purchase and rental of exploits and exploit kits that fuel an enormous number of infections across the world.

When we read about data breaches, the cybercrime industry may seem so far removed from everyday life that it is tempting to ignore the message. However, cybercrime is merely an evolution of traditional crime. We must conquer our apathy and pay attention to advice for fighting malware and other threats. Otherwise, information from our digital lives may appear for resale to anyone with an Internet connection. When it comes to medical data, however, the ability to recover our information is considerably harder than with other data. For example, when retail store Target was breached in 2013, **victims had their compromised cards cancelled and new payment cards reissued**. This limited the damage to individuals because the cards flooded the underground market and were quickly offered for sale. For medical data, and personal information, the recovery strategy is not quite as simple. Thus it is imperative that we take proactive measures to reduce the probability of such data being stolen.

One troublesome issue with this topic is the lack of evidence pointing to the motivation behind the acquisition of stolen medical data. With payment card information we have documented that stolen card numbers are used to conduct fraud against the victims. In the course of our investigations we have identified where specific data is sought to verify the addresses of the victims. At present, however, we have not identified specific uses for bulk data purchases of medical data. We will continue our research on this topic because it deserves significant attention, and will post updates as we find more data.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com