SecurityScorecard DARKOWL

Listening to Patient Data Security: Healthcare Industry and Telehealth Cybersecurity Risks

SecurityScorecard and DarkOwl 2020 Healthcare Report

securityscorecard.com [800] 682 1707

SecurityScorecard

Table of Contents

DARKOWL

Overview

With the onset of the COVID-19 pandemic, cybersecurity's focus turns once again to the healthcare industry. While COVID-19 has proven the healthcare industry's overall resilience, the research found it has also increased its cybersecurity risk with new and emerging threats. The rapid adoption and onboarding of telehealth vendors led to a significantly increased digital footprint and attack surface, leaving both provider and patient data at risk. The good news for providers in this year's healthcare industry report is that, as a whole, security posture improved compared to the SecurityScorecard 2019 report.

As of July 23, 2020, the U.S. Department of Health and Human Services (HHS), the agency tasked with monitoring compliance with the Health Insurance Portability and Accountability Act (HIPAA), renewed its declaration that a Public Health Emergency exists,[1] extending the timeframe for the "Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency."[2] While this moratorium on requiring compliance with certain Privacy Rule requirements provides the healthcare industry some necessary breathing room, the document notes specifically:

> "In an emergency situation, covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures. Further, covered entities (and their business associates) must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information."

The 'Limited Waiver' relaxes HIPAA provisions such as sharing information with family members and collecting patient consent for information sharing. However, the document maintains that all other cybersecurity requirements, under the Security Rule, remain in effect.

In conjunction, the COVID-19 pandemic accelerated healthcare providers' use of telehealth applications as a way to mitigate patient physical health risk by providing contactless treatment. According to a brief from the U.S. Department of Health and Human Services, at the height of the pandemic, the number of telehealth primary care visits increased 350-fold from pre-pandemic levels. The immediacy of the shift to telehealth not only increased healthcare providers' digital footprints, but it also created a time crunch, making traditional vendor risk management practices and oversight a barrier to providing the best patient healthcare possible.

This year, SecurityScorecard partnered with DarkOwl, a leading dark web research company, to bring not only insights about the cybersecurity risks of telehealth but also an inside look at the way real cybercriminals are discussing electronically protected health information (ePHI).

[1] Azar, Alex. (2020). "Renewal of Determination That a Public Health Emergency Exists." Department of Health and Human Services. July 23, 2020. https://www.phe.gov/emergency/news/healthactions/phe/Pages/covid19-23June2020.aspx

[2] Department of Health and Human Services. (2020). "Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency." https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf

Key Insights on Cybersecurity for Healthcare and Telehealth Organizations

Over the past four years, SecurityScorecard has reported on the cybersecurity struggles the healthcare industry faces. In this year's report, SecurityScorecard and DarkOwl looked at over one million organizations — over 30,000 in healthcare alone — from September 2019 to April 2020 and analyzed terabytes of information to assess risk across 10 factors.

The healthcare industry, despite new risks from telehealth vendors, slightly improved its security posture compared to 2019. The industry moved to 9th place out of 18 reviewed industries (up from 10th in 2019.) This is heartening, especially as the industry has been overwhelmed by an influx of patients, limited resources, rationing, and other challenges due to COVID-19. Several key factors lead to the new ranking:

Improving to 4th from 10th for **patching cadence**

Maintaining 5th ranking for **network security**

Maintaining 8th ranking for **application security**

There was a slight decrease in rank for DNS health (slipping to 14th from 13th) despite a general improvement in DNS health and for endpoint security (moving from 12th to 13th), but overall, the impact of the improvements in other categories carried more weight in the rankings, such as patching, one of the most critical security controls used to mitigate cyberattacks. It's clear from the strides made that the healthcare industry is dedicated to securing patient information.

Interestingly, malware infections reported within SecurityScorecard's IP Reputation category saw a 77% decrease in findings for the healthcare industry overall, indicating that the healthcare industry as a whole is taking more steps to reduce the compromise of endpoints within their internal networks than in previous years. Additionally, the increase of the healthcare industry's attack surface has expanded due to remote working conditions - which could also indicate a shift in focus from the standpoint of attackers. In other words, with the majority of healthcare organizations working with limited staffing, cybercriminals may have chosen to target home networks rather than organizational networks, as has been observed in other industries.

Despite this overall improvement, one area in healthcare does bring more risk: telehealth vendors and the digital supply chain that supports them. As a result of a massive usage spike to maintain social distancing during the pandemic, telehealth providers experienced a surge in targeted attacks. SecurityScorecard focused its 2020 efforts on reviewing the 148 most-used telehealth vendors according to Becker's Hospital Review. SecurityScorecard's research team looked at the percentage increase in findings, or security alerts sent to IT staff. The research compared the findings for the period of September 2019 through February 2020 to those for the period of March through April of 2020.

The key takeaway of the 2020 report is that telehealth providers have experienced a nearly exponential increase in targeted attacks as popularity skyrocketed, including a 30% increase of cybersecurity findings per domain, notably:

117% increase in IP reputation security alerts

- Malware infections — as part of successful phishing attempts and other attack vectors — ultimately cause IP reputation finding issues

65% increase in patching cadence findings

- Patching cadence is the regularity of installing security patches and is often one of the primary security policies that protect data

56% increase in endpoint security findings

- Exploited vulnerabilities in endpoint security enable data theft

16% increase in application security findings

- Patients connect with telehealth providers using web-based applications including structured and unstructured data

42% increase in FTP issues

- FTP is an insecure network protocol that enables information to travel between a client and a server on a network. FTP has been more in use since remote work has become more prevalent

27% increase in RDP issues

- RDP is a protocol that allows for remote connections between users in different locations, which has seen increased usage since the widespread adoption of remote work

The increased IP address reputation findings for telehealth vendors is the starkest difference: while the overall healthcare industry saw a 77% decrease in findings, the same incidents in telehealth increased by 117%. This appears to reinforce the hypothesis that cybercriminals moved away from targeting healthcare organization networks to focus on the third party supply chain vendors' network security instead.

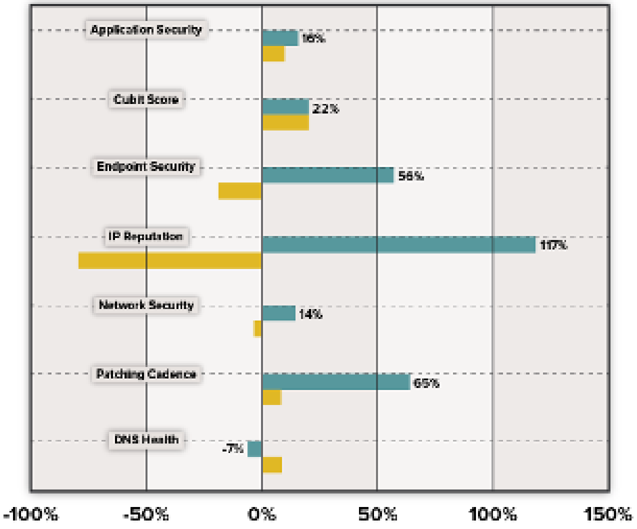
Healthcare Security Improvements Prior to COVID-19

Prior to COVID-19 overwhelming the healthcare industry in the U.S., healthcare organizations and business associates worked tirelessly to protect health data with the same rigor as they protect physical health. A look at the cybersecurity improvements between the 2019 report and 2020 report shows that the healthcare industry's security treatments were helping to improve their IT health.

🟨 Before covid = September 2019 to February 2020 Healthcare Change

🟦 Before covid = September 2019 to February 2020 TeleHealth Change

Percent Change in Mean Findings Before March (Covid) and After



Application Security

The healthcare industry increased its application security posture by 10% in the last year while simultaneously increasing use.

Patients connect with telehealth providers using web-based applications including structured and unstructured data. A survey published by the American Medical Association (AMA) in February 2020 noted that medical professionals increasingly used applications for telehealth, virtual visits, and remote monitoring to improve patient safety and medical care efficiency.[3] Even before COVID-19 forced most healthcare professionals to embrace these technologies, patients and physicians were already moving toward digital health tools. For example, according to the AMA survey, use of mobile applications and wearables for chronic illness patients increased from 13% in 2016 to 22% in 2019.[4]

This widespread use of mobile applications and digital health technology further emphasizes the importance of application security overall. Protecting data means ensuring that all access points, specifically those in the cloud via mobile applications, have robust security controls.

Patching Cadence

Taking to heart the last few years of security research, the healthcare industry improved its overall score for patching cadence by 10%.

Patching cadence, or the regularity of installing security patches, is often one of the primary security controls that protect data. According to an article from CSO, 60% of data breaches involved known vulnerabilities for which a security patch was available.[5] A March 2020 report by the International Medical Device Regulators Forum (IMDRF) explains that part

[3] Miliard, Mike. (2020) "AMA sees surge in health IT adoption, 'rise of the digital native physician'." Healthcare IT News, February 6, 2020.

[4] Ibid.

[5] Fruhlinger, Josh. (2020). "Top cybersecurity facts, figures and statistics for 2020." CSOOnline.com. March 9, 2020.

of a Total Product Life Cycle Cybersecurity Management Plan includes a "plan outlining how software will be updated or how other remediation actions would be applied to maintain ongoing safety and performance of the device either regularly or in response to an identified vulnerability."[6] Manufacturers need to consider how the devices they design can be updated to mitigate risks associated with outdated software, but healthcare professionals share in the cybersecurity responsibility.

According to the Forrester Wave Leader 2020 "Connected Medical Device Security" report, connected medical devices can constitute up to 74% of the devices on a hospital's network. With that in mind, the healthcare industry's increased patching cadence score provides a greater level of confidence over its attention to data security and privacy this year compared to last year.

DNS Health

As with both application security and patching cadence, the healthcare industry improved its DNS health score by 10% in the last year.

DNS servers act as the interpreter between a website's numerical IP address and the more commonly understood URL. DNS hijacking is one method cybercriminals use to gain access to systems and networks. By compromising a DNS server, malicious actors can alter IP addresses in a database as part of a malware attack. In fact, on July 16, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released an emergency directive indicating that despite not finding any active exploitation of a Microsoft Windows Server vulnerability, "it is only a matter of time for an exploit to be created for this vulnerability."[7] CISA also noted that several mitigation strategies include vulnerability scanning and web application scanning. Moreover, the interconnectedness of digital transformation shows that no single risk factor exists in a vacuum since the final line of the directive states, "If you have Windows Servers running DNS, you should patch now. Don't wait on this one."[8]

In short, the DNS health score improvement highlights the healthcare industry's proactive approach to cybersecurity.

Cybersecurity, Telehealth and COVID-19

Although the healthcare industry as a whole improved between 2019 and 2020, COVID-19 forced a rapid move to telehealth for non-coronavirus patient care as a best practice for responding to the declared Public Health Emergency (PHE). This shift led many healthcare organizations to adopt

[6] Medical Device Cybersecurity Working Group. (2020). "Principles and Practices for Medical Device Cybersecurity." International Medical Device Regulators Forum. March 18, 2020. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

[7] Krebs, Christopher. (2020). "Emergency Directive (ED 20-03) Windows DNS Server Vulnerability." Cybersecurity and Infrastructure Security Agency. July 16, 2020. https://www.cisa.gov/blog/2020/07/16/emergency-directive-ed-20-03-windows-dns-server-vulnerability

[8] Ibid.

third-party telehealth providers en masse, often without the time to engage in critical vendor risk management processes.

According to the July 28, 2020 HHS issue brief titled “Medicare Beneficiary Use of Telehealth Visits: Early Data from the Start of the COVID-19 Pandemic, “nearly half (43.5%) of Medicare primary care visits were provided via telehealth in April, compared with less than one percent before the PHE in February (0.1%).”[9] Meanwhile, the Centers for Disease Control continues to support the use of telehealth services as a way to reduce staff exposure to ill patients, preserve personal protective equipment (PPE) and reduce the number of patients flooding facilities.[10]

Although healthcare professionals may be protecting physical health by using telehealth services, they also need to ensure they are not putting data health at risk instead. From a dark web perspective, DarkOwl has knowledge of multiple organizations that have been breached during the pandemic that would likely include patient data and/or diagnostic research. DarkOwl has also noted an increase in the use of ransomware as a service (RaaS) in 2020 and throughout the pandemic, with the healthcare industry emerging as notable dark web target.

In one case in late June, cybercriminals used a strain of ransomware known as Netwalker to compromise the University of California San Francisco’s (UCSF) internal networks. According to open sources, the dark web posting from the hackers contained screenshots with files stolen from UCSF, with references to the US Centers for Disease Control and Prevention and UCSF departments tied to COVID-19 research.[11]

Threat actors have recently successfully used COVID-related content in phishing emails to get victims to click on malicious links. In early July 2020, the Netwalker team posted data for a Pennsylvania based medical group (Crozer-Keystone Health System) that they allegedly stole using such a phishing attack, but details about the data accessed is unavailable and the compromise has not been publicly disclosed.

Notable Increase of Telemedicine Vulnerabilities

Telemedicine vendors are integral to providing the best patient care possible. As business associates, the healthcare industry needs visibility into the increased cybersecurity vendor risks that telehealth providers bring to the IT ecosystem.

While the industry has increased its security posture over the last year, SecurityScorecard’s research notes that the accelerated onboarding of telehealth providers has also increased ecosystem risks.

[9] Office of the Assistant Secretary for Planning and Evaluation. (2020). "Medicare Beneficiary Use of Telehealth Visits: Early Data from the Start of the COVID-19 Pandemic." US Department of Health and Human Services. July 2020. https://aspe.hhs.gov/system/files/pdf/263866/HP_IssueBrief_MedicareTelehealth_final7.29.20.pdf

[10] Centers for Disease Control. (2020). "Using Telehealth Services." June 10, 2020. https://www.cdc.gov/coronavirus/2019-ncov/hcp/telehealth.html

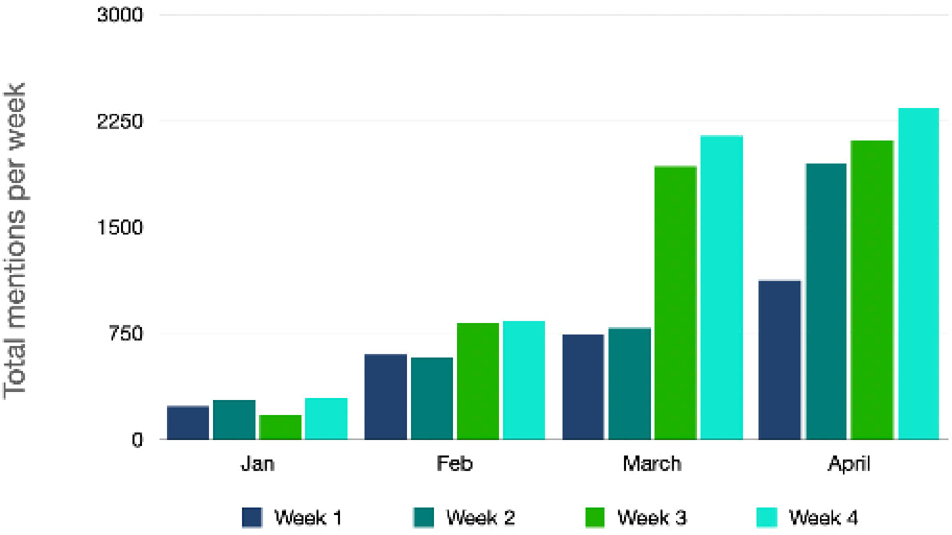
[11] HeathIT Security (2020). "UCSF Pays $1.14M to NetWalker Hackers After Ransomware Attack" https://healthitsecurity.com/news/ucsf-pays-1.14m-to-netwalker-hackers-after-ransomware-attack

SecurityScorecard's findings note increased risks across the following factors:

Application security, endpoint security, IP reputation, and patching cadence saw most significant increases in weaknesses detected

Network security risks, while increased, had a less noticeable incline from the previous period

Notable Increase of Telemedicine Companies in Dark Web Records



DarkOwl's research further reveals increased vulnerabilities to ePHI. Since the onset of the pandemic, DarkOwl observed a notable increase in mentions of the top 20 telemedicine companies on the dark web.

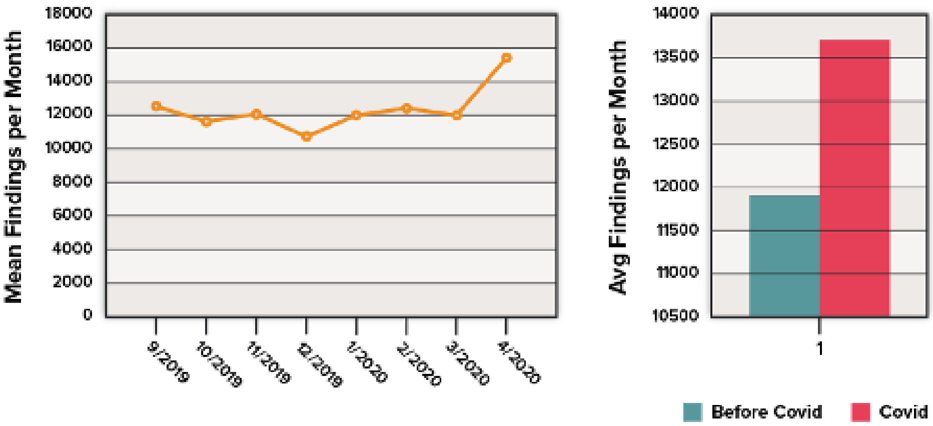
Using their Vision platform, a searchable database of dark web data from underground marketplaces, forums and anonymous hidden services, DarkOwl researchers analyzed current and historical content by scraping the extensive dark web and deep web sites. The team then focused on assessing the extent of hacker chatter about the top 20 telehealth companies. DarkOwl analysts reviewed the volume of documents containing mentions of these companies, reviewing each week individually, from the start of January to the end of April 2020.

During this time, DarkOwl noticed a significant upward trend in the number of results containing these terms from their dark web database. The starkest increase in mentions of telehealth keywords was observed from the second to the third week of March when there was a 144% increase.

Using DarkOwl Vision's crawl date feature, analysts reviewed the volume of documents containing mentions of the top 20 telehealth/telemedicine companies for the above mentioned period and review process. For each of the weeks reviewed, queries researched for mentions of any of the following phrases: "*CareClix*," "*ConsultADoctor*," "*Teladoc*," "*MeMD*," "*iCliniq*," "*American Well*," "*MDAligne*," "*StatDoctors*," "*Doctor on Demand*," "*Specialists On Call*," "*LiveHealth Online*," "*Virtuwell*," "*Ringadoc*," "*PlushCare*," "*HealthTap*," and "*HealthExpress*."

Telehealth Third-Party Security and Dark Net Research Findings

Application Security



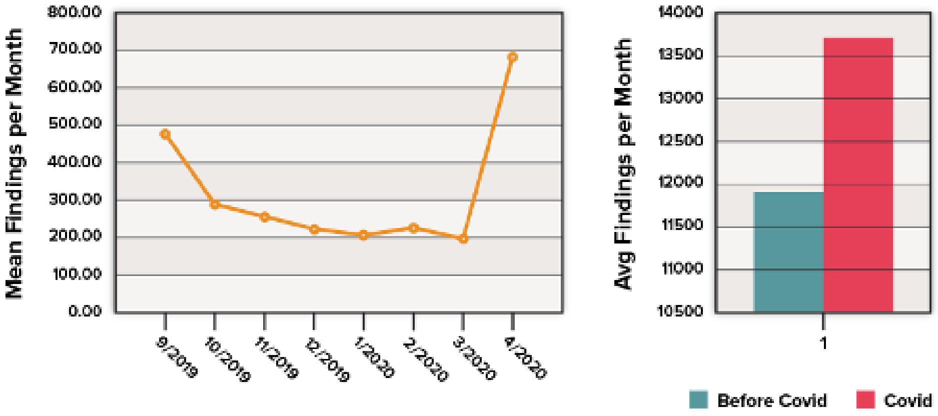
SecurityScorecard's research indicated a steep incline in the number of application security weaknesses for telehealth providers.

Patients connect with telehealth providers using web-based applications that include structured and unstructured data. With the exponential increase in use of these applications, cybercriminals targeted them more purposefully.

DarkOwl's research supports the connection between application security and the increased presence of ePHI on the dark and deep web. For example, in March, DarkOwl observed cybercriminals openly distributing and discussing sensitive patient records on a RaidForum's subgroup, utilizing the encrypted chat application, Telegram.

The sharing of patient records strongly indicates that the web applications storing the data were vulnerable to malicious attacks. Ultimately, the inability to gain visibility into these risks increased the negative impact of telehealth on patient data security and privacy.

Endpoint Security



Endpoint security vulnerabilities increased even more steeply than web application vulnerabilities.

As part of telehealth initiatives, the Food and Drug Administration (FDA) issued and reissued an Emergency Use Authorization (EUA) for certain medical devices. Reissued on July 14, 2020, the notice indicates that the pandemic as a public health emergency supports the emergency use of COVID detection/diagnostic devices, personal respiratory protective devices, and medical devices.[12] These devices enable remote connections between patients and healthcare providers while reducing contact, ultimately helping to limit the spread of COVID-19. However, the they also create data security and privacy risks as malicious actors attempt to infiltrate the devices to obtain health information.

Supporting the importance of endpoint security as an ePHI protection, DarkOwl's research indicates that exploited vulnerabilities enable data theft. In late April, a hacker using the moniker bzyo detailed the specifics on how to cause a critical buffer overflow in Rubo Medical's DICOM Viewer imaging software version 2.0. The hacker debuted the python-based exploit on Windows 7 operating system with SP1.

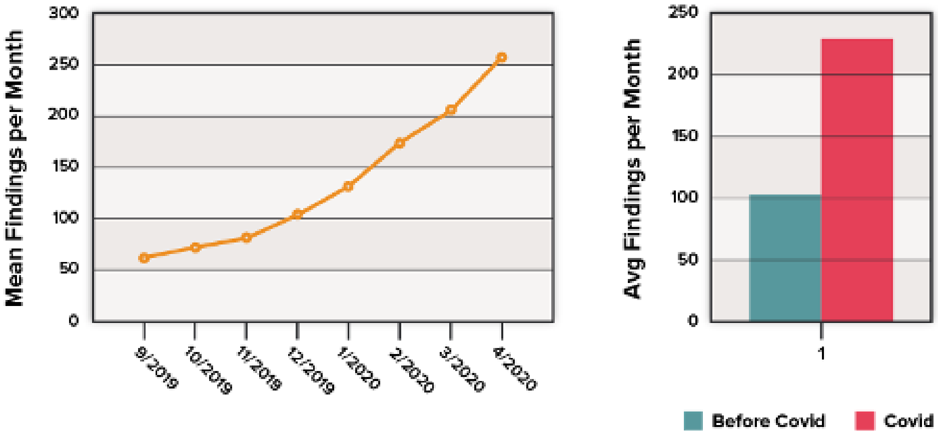
DICOM stands for Digital Imaging and Communications in Medicine, which is the standard for the communication and management of medical imaging information, a common communications architecture across numerous medical devices that rely on imaging and digital data protocols.

Vulnerable servers with the DICOM communication protocol could potentially be subject to a man-in-the-middle (MITM) attack resulting in manipulated imagery and falsified medical imaging documents. Exploiting this vulnerability could lead to the transmission and download of digital images (such as X-rays) which could then enable malicious actors to alter or sell the data.

[12] Food and Drug Administration. (2020). "Authorization of Emergency Use of Certain Medical Devices During COVID-19; Availability." Federal Register. July 14, 2020. https://www.federalregister.gov/documents/2020/07/14/2020-15137/authorization-of-emergency-use-of-certain-medical-devices-during-covid-19-availability

Endpoint security vulnerability is one of the largest problems facing the medical community's adoption of telehealth services since stay-at-home orders have become the ultimate experiment in "bring your device to work" security.

IP Address Reputation



IP reputation vulnerabilities saw a steadier, as opposed to sharper, increase as part of the telehealth pivot.

Successful phishing attempts that lead to malware infections directly impact IP reputation issues. This has been an ongoing data health crisis running in tandem with the public health crisis. For example, in April 2020, the National Cyber Awareness System posted an alert that malicious actors started focusing on COVID-related phishing attacks such as the "CovidLock" malicious Android app purporting to provide real-time coronavirus outbreak tracking and in email attachments with phrases such as "Coronavirus Update" or "2019-nCov: Coronavirus outbreak in your city (Emergency)."[13] Whether it comes from successful phishing attacks or other methodologies, medical device vulnerability has critical implications for telehealth data privacy.

SecurityScorecard saw that malware in IP attribution rose by 117% for telehealth organizations. In addition, the research showed an increase in malware activity among telehealth organizations, but an overall decrease in the healthcare industry, indicating that malware has most likely shifted from healthcare offices to residential IP addresses. Across the research, malware findings were reduced by 10% on "lockdown" office IP addresses while there was a 30% increased in residential IP's. During the 2018 government shutdown, SecurityScorecard witnessed a very similar finding.

SecurityScorecard's research also indicated an increase in FTP issues (up 42%) and RDP issues (up 27%), which are likely tied to remote work. FTP refers to the network protocol that enables information to travel between a

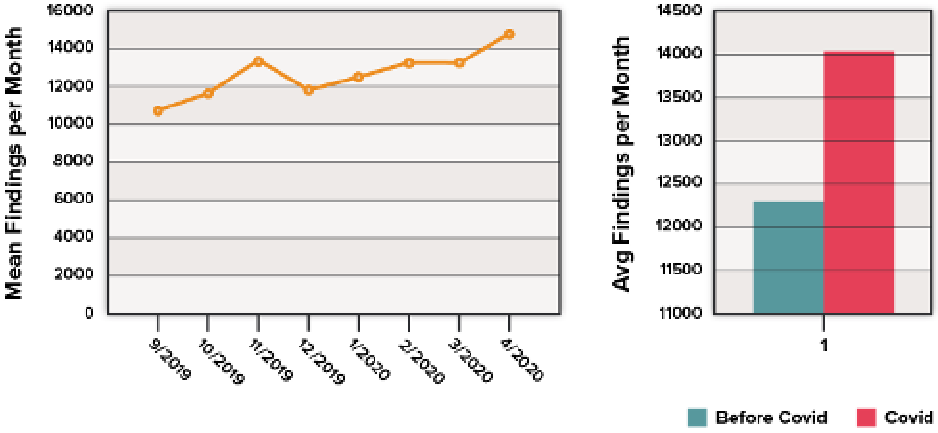
[13] Cybersecurity and Infrastructure Security Agency. (2020). "Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors." Cybersecurity and Infrastructure Security Agency (CISA). April 8, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-099a

client and server on a network. RDP is a Microsoft proprietary protocol that allows one user to connect to another user's computer such as when remote workers request IT help desk services. Businesses have likely enabled FTP and RDP to allow remote workers access to corporate assets or files from their homes or other places of residence. In the best of times, many healthcare organizations would normally have enabled these by putting them behind a VPN or some other authentication system. With limited time to make drastic changes to remote work, organizations also exposed them to the internet — which enabled remote work but also created a significant attack surface increase. Exposed RDP on the internet continues to be the most exploited vector for ransomware attacks.

Comparing this with the DarkOwl data once again gives insight into the negative impact that these increased vulnerabilities have on patients' data protection. The hacker using the moniker TheDarkOverlord is well known for targeting ePHI, then packaging and reselling it to other cybercriminals. In 2016, they obtained thousands of healthcare records from three different US-based organizations they successfully penetrated via an "exploit in how companies use RDP" along with readily available plaintext usernames and passwords. The data was offered for sale on a dark web marketplace, with prices ranging from $100K to 300K USD in cryptocurrency. As of January 2019, the lone hacker has expanded into a team of criminals who are still offering terabytes (TBs) of breached medical data to willing buyers.

The accelerated adoption of telehealth services that rely on web-based connectivity and RDP indicates that this risk factor should be a priority when evaluating third-party telehealth provider risk.

Network Security



Network security risks increased at a slower rate than other risks during the review period, which likely arises from telehealth vendors leveraging home networks as opposed to in-office networks. While malicious actors continued to target corporate telehealth networks, the majority went unused because of stay-at-home orders. It's worth noting that the attempted attacks on corporate networks did not stop completely, perhaps in an effort to take advantage fewer people managing the security on-premises, open access points, and/or database vulnerabilities.

With relaxed firewall rules to enable telehealth services and IT staff working remotely, network security acts as an additional threat vector as evidenced by dark web research. According to DarkOwl, one of the dark web's current most prolific hackers, spectre, regularly drops large datasets from commercial and government institutions on their personal hidden service on Tor, an open-source browser known to conceal users' identity which makes it a popular location for malicious actors to connect to one another.

> Over the last year, the infamous dark web threat actor has released the records of a number of major medical providers and their patients, including a large healthcare organization based in the Midwest United States. SQL injection is spectre's weapon of choice as much of the raw data consists of exported tables from the medical records' SQL database.

Meanwhile, in early March 2020, another hacker using the moniker *Data_Baron* offered 280 databases for sale on popular underground forum RaidForums. The list of databases included medical records from a number of countries, such as:

"Mongolia 450.106 Medical Records"

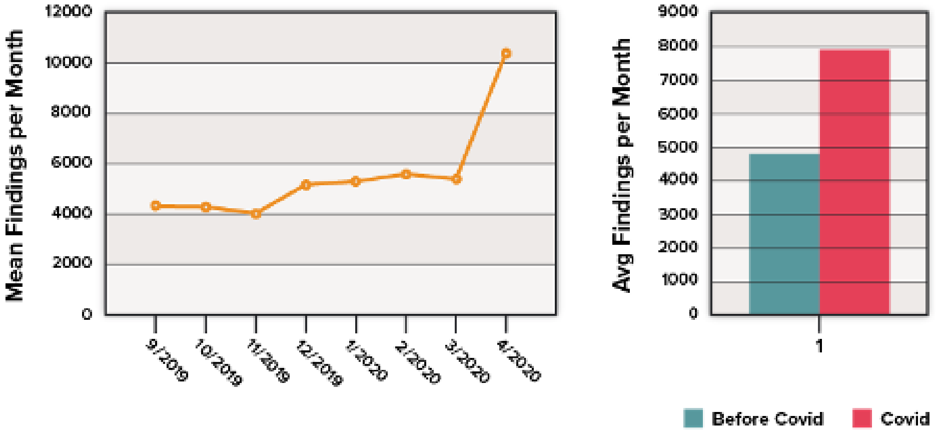
"Egypt 5.22.570 Medical Records"and

"PeruHealthInsurance 3.581.822 Medical Records"

Another five databases are listed as "ThaiMedical" from 2011. Like many other cybercriminals on the dark web, the preferred method of contact is encrypted XMPP/Jabber or Telegram.

This data, downloaded from insecure network-connected databases highlights the problems associated with securing cloud-storage and network security vulnerabilities.

Patching Cadence



Another large spike in observed vulnerabilities exists in the area of patching cadence, which remains one of the most important security controls. In a report published in August 2020, analyst firm McKinsey lists patching first in the required controls organizations need to put into place. According to the report, "shortening patch cycles for systems, such as virtual private networks (VPNs), end-point protection and cloud interfaces that are essential for remote working will help companies eliminate vulnerabilities soon after their discovery. Patches that protect remote infrastructure deserve particular attention."[14] Although focused primarily on remote workforce security needs, telehealth services are healthcare's version of conference calls. To truly secure telehealth, healthcare providers need to incorporate patching cadence as an integral part of their vendor due diligence.

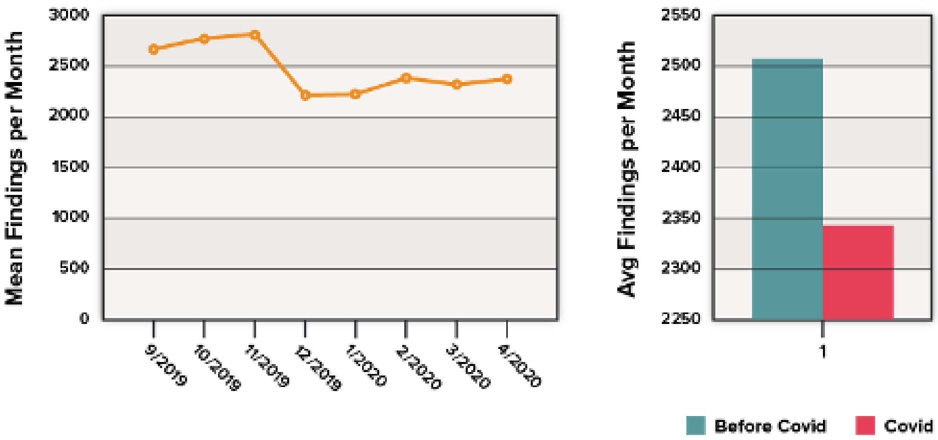
As one of the primary cyberattack risk factors, less frequent security patch updates lead to greater data theft risk. DarkOwl's research indicates that in early January 2020, a Russian cybercriminal expressed interest in obtaining electronic medical record data on a popular dark web forum. The hacker specifically mentioned "Advanced MD," a popular cloud-based medical office software application that supports everything from electronic patient records to telemedicine-based appointments.

The open-source patient record system used by the UK, *OpenEMR*, is also of high concern. In particular, this telehealth software is regularly discussed and targeted on the dark web. Adding to this concern, DarkOwl Vision collected source code from a temporary pastesite that suggests that hackers have attempted to access MYSQL databases within OpenEMR's system and likely continue to do so.

As healthcare providers look to secure their telehealth vendor ecosystem, they need greater visibility into how their business associates prioritize updates and how often they apply security patches.

[14] McKinsey & Company. "McKinsey on Risk Special Edition :The COVID-19 Crisis." McKinsey. August 2020. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/McKinsey%20on%20Risk%20Special%20issue%20on%20the%20COVID%2019%20crisis/MoRisk-COVID-FINAL.pdf

DNS Health: Testing Negative for Risk



DNS health is the only area that saw a decrease in the number of vulnerability findings.

Recognizing that most telehealth services operate over unprotected networks, most organizations likely sought to mitigate the risks by securing their DNS health. For example, one of the easier ways to steal data is through DNS spoofing or DNS hijacking. Cybercriminals alter the communications between a user's browser and the DNS server that translates the URL, then leverage that redirected communication to steal credentials.

Understanding the devastating impact that DNS spoofing can have on patients, many organizations appear to have increased their DNS health to prevent these attacks.

The Value of Security Ratings in Healthcare

Security ratings provide organizations with critical intelligence about their security posture and the security posture of their overarching ecosystem. In 2019, leading analyst firm Gartner highlighted the value of security ratings noting that to mitigate risks across complex ecosystems, "SRM leaders should leverage security rating services (SRS) as an additional data point to provide continuous, real-time scoring for their overall digital ecosystem at a low cost in terms of effort, labor, and capital. Security rating services provide continuous, independent, and quantitative technical analysis and scoring for public-facing digital assets of organizational entities across geographies."[15]

[15] Olayei, Sam, Peter Firstbrook, Briand Reed, Prateek Bhajanka, and Neil MacDonald. "Top 10 Security Projects for 2019." Gartner February 11, 2019. https://www.gartner.com/en/documents/3900996/top-10-security-projects-for-2019

Security ratings provide an “outside-in” view of an organization’s security posture. Continuous controls monitoring includes active and passive scanning capabilities such as scans, data feeds, honeypots, and sinkholes. These ratings platforms offer visibility into the same types of hidden risks that cybercriminals use to steal information.

They also provide at-a-glance insight into how well an organization is maintaining mission-critical security, privacy, and compliance controls. The higher the organization’s score, the more robust its security posture. Additionally, security ratings provide real-time, actionable alerts that enable a proactive approach to managing cybersecurity.

The Value of Dark Web Research in Healthcare

This year, SecurityScorecard partnered with DarkOwl to provide greater insight into the types of information shared on the dark web and how cybercriminals share data. By looking at the dark web in conjunction with other security assessments, healthcare and telehealth companies gain a significantly more informed picture of their overall threat landscape. This is largely because, for years, cybercriminals have targeted patient medical records and electronic medical systems and have exchanged information pertaining to these exploits in dark web marketplaces and forums.

Overall, DarkOwl saw a noticeable increase in mentions of major healthcare and telehealth companies across the dark web since February 2020. In investigating telehealth companies on the dark web as part of this research, DarkOwl discovered evidence of prolific and emerging threat actors selling electronic patient healthcare data, malware toolkits that specifically target telehealth technologies, and strains of ransomware that are uniquely configured to take down healthcare IT infrastructure.

Furthermore, as a result of the coronavirus pandemic, dark web research indicates an increased risk to the healthcare systems, specifically through medical device system vulnerabilities and targeted attacks on the information in their databases. Evidence of emerging threat actors indicates that new cybercriminals are entering the healthcare data selling space which ultimately leads to new risks facing healthcare organizations and their IT supply stream.

By understanding malicious actors' methodologies, organizations can proactively mitigate risks and detect potential data leaks. For this reason, considering the dark web when looking at the cyber threat landscape of the healthcare and telehealth industries provides insight into how threat actors see these industries as targets and enables threat protection teams to remain one step ahead of potential attackers.

SecurityScorecard and DarkOwl: Full Visibility into Risk Mitigation

Securing healthcare data is a persistent challenge. Every day, new information seems to undermine an organization's current controls; the ability to pivot rapidly in response to changes in their environment is critical. As the healthcare industry embraces telehealth in the long term, providers and business associates need the tools necessary to continue to prevent data health threats.

Bringing together security ratings and dark web research can provide the necessary information to make informed cybersecurity decisions. With SecurityScorecard's security ratings platform, healthcare organizations gain real-time visibility to control weaknesses and mitigate risks across the interconnected vendor ecosystem. SecurityScorecard's platform monitors cybersecurity posture across 10 risk factor categories using an A through F rating scale. Its research shows that organizations with a rating of C, D, or F are five times more likely to experience a data security incident. Using SecurityScorecard's cloud-based ratings system, healthcare organizations can rapidly gain insight into their own cyber risks as well as those throughout their ecosystem.

DarkOwl enhances continuous controls monitoring by leveraging threat actor discussions on the dark web to help predict their next targeted attack vectors. Understanding the discussions on the dark web gives greater insight into how threat actors are evolving and targeting telehealth companies, thus enabling healthcare organizations and business associates to better prioritize their cybersecurity activities. DarkOwl data provided throughout this report was sourced from DarkOwl's Vision database of darknet content, which is collected from sources such as Tor, I2P, Telegram, IRC, authenticated chat rooms, Zeronet, and more. DarkOwl employs a team of research analysts who draw from additional deep web and surface web sources that have been cross-referenced with intelligence gained from first-hand darknet data reconnaissance to present these findings with a high degree of confidence.

Malicious actors will continue to target the healthcare industry's sensitive data. In today's environment, defense in depth requires more than a single tool. A combination of security tools that provides visibility into the robustness of controls as well as potential data leakage strengthens an organization's proactive and reactive responses to protecting patient information.Together, SecurityScorecard and DarkOwl provide the necessary outside-in view of a company's cybersecurity controls from the cybercriminal's technical and human side.

For more information about how these tools can help heal your cybersecurity program, contact SecurityScorecard and DarkOwl today.

About SecurityScorecard

SecurityScorecard is the global leader in cybersecurity ratings and the only service with over a million companies continuously rated. Founded in 2013 by security and risk experts Dr. Alex Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 1,000+ organizations for self-monitoring, third-party risk management, board reporting and cyber insurance underwriting; making all organizations more resilient by allowing them to easily find and fix cybersecurity risks across their externally facing digital footprint. SecurityScorecard is the only provider of instant risk ratings that automatically map to vendor cybersecurity questionnaire responses - providing a true 360- degree view of risk. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every company has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

To receive an email with your company's current score,
please visit instant.securityscorecard.com.

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.io

SecurityScorecard HQ
111 West 33rd Street
11th Floor
New York City, NY 10001

securityscorecard.com

[800] 682 1707