Malwarebytes

eBOOK

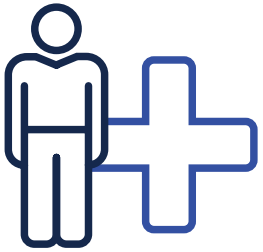
What cybercriminals want from your healthcare organization

Introduction

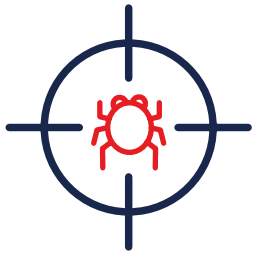
Cybercriminals target the medical industry for a gold mine of personal and financial data.

As 21st century health records have moved from paper to digital and as the healthcare infrastructure handling smart medical devices and network-connected systems has become increasingly complex, cybercriminals have taken note. Unfortunately, while the personally identifiable information (PII) stored on endpoints is valuable to patients, physicians, and healthcare providers, it's also highly sought after by cybercriminals.

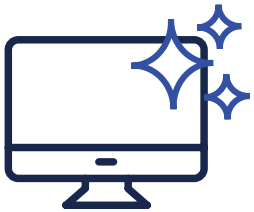
Unlike stolen credit cards, electronic patient records contain PII that never expires, which can be repeatedly used for malicious intent. With stolen PII, criminals can falsify insurance claims and tax returns, obtain fraudulent credit cards, open bank accounts to write bad checks, and obtain government-issued passports to create new identities. The opportunities are endless.



Every day, the medical sector is exposed to cyberthreats like Trojans, ransomware, insider threats, and other forms of malware—with the most disruptive coming from information-stealing Trojans and ransomware attacks. Threat detections have increased from about 14,000 healthcare-facing endpoint detections in Q2 2019 to more than 20,000 in Q3, a growth rate of 45 percent.[1]



In 2020, healthcare organizations remained a target. In April, the international law enforcement agency Interpol warned that, amidst the broader global pandemic, hackers were targeting healthcare systems with ransomware. The agency's warning came just days after Microsoft told several dozen hospitals that their gateway and VPN appliances were vulnerable to attacks.



1. Malwarebytes. Cybercrime Tactics and Techniques: the 2019 state of healthcare. November 2019.

For healthcare organizations to effectively implement security measures unique to their environment, they must first understand why cybercriminals are trying to breach their networks. This paper identifies the top four healthcare targets for cybercriminals and the impact of their compromise on medical staff, patients, and daily operations.

Top 4

healthcare targets for cybercriminals

1. Patient PII
2. Operations, systems and files for ransom
3. Technology providers, vendors and suppliers
4. Broad attack surface

1

Patient PII

While some healthcare organizations have opted to house pertinent patient and medical data they keep on record in the cloud, many choose to store theirs locally. Per patient, they store a wide range of PII that's valuable to a criminal to orchestrate identity theft, such as name, date of birth, home address, email address, and Social Security number (SSN).

Then there's the wealth of electronic protected health information (ePHI) that the medical sector stores on each patient, including health records, images from medical exams, blood tests and other test results, as well as diagnosis and treatment information. Combined with stolen PII, when bad actors gain access to patient records, they have, in essence, a goldmine to commit insurance fraud.

Target 1

Cybercriminals can sell information deemed valuable either individually or as a data set, which underground criminals refer to as "fullz"—a selling jargon that means the full identity package of a person. **Patient data is highly sought after by cybercriminals. In fact, healthcare records fetch a high price with individual records commanding $1,000 on the dark web.**[2]

That's a lot of financial profit for cybercriminals, and, unfortunately, stolen records come at a steep cost for the medical sector. **Healthcare organizations have the highest industry costs associated with data breaches at $6.45 million—65 percent higher than the global average of all industries.**[3] Healthcare costs rank well above other industries because the sector experiences an average total cost per stolen record of $429, which is significantly higher than less regulated industries.

2. Becker's Health IT & CIO Report. Patient medical records sell for $1k on the dark web. 2019.
3. Ponemon. Cost of a Data Breach Report. 2019.

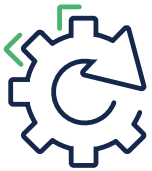
Target 1

Impact of PII theft on patients and staff

A cybercriminal owning a single data set on a patient or a staff member working in a healthcare organization can fully take over their identities by posing as them when dealing with governments and private institutions, whether that's for tax purposes or taking out a loan.

They can also mix up or combine certain data to create a new identity profile. These new profiles are called "synthetic identities," which is the fastest growing financial crime.[4]

4. Forbes. Synthetic Identity Fraud Is The Fastest Growing Financial Crime. October 2019.



Operations, systems, and files for ransom

The healthcare sector is an essential critical infrastructure entity that must remain operational around-the-clock to serve the local community and surrounding region. This makes ransomware attacks especially dangerous to the healthcare industry with the risk of causing significant financial, reputational, health, and safety harm.

Ransomware attacks usually deny access to the healthcare organization's systems and files until a ransom is paid. And in the event it isn't paid, some attackers may threaten to sell the "captured" PII on the black market. Ransomware accounts for most healthcare malware attacks. And when they hit, they cripple operations. Life-saving surgeries must be postponed, appointments canceled, and medical tests halted. It's safe to say that the consequences of ransomware for the healthcare industry far outweigh any other organization, as essential devices, systems, and files are locked out.

2

Target 2

Impact of ransomware on healthcare

Even with lives on the line, cybercriminals are not showing any signs of mercy with their ransomware attacks on the medical sector. According to analysis by Coveware, not only did the average ransomware demand rise 184 percent to $36,295, but the healthcare industry accounted for 13.6 percent of ransomware targets.[5] In addition to the cost of paying the ransom (if the organization makes that decision), impacted organizations must notify patients of the data breach and inform them that their information may have been exposed.

And, what better way to demonstrate the impact ransomware has on healthcare operations than to share some examples that occurred in 2019 and 2020?

5. Coveware. Ransomware Amounts Rise 3X in Q2 as Ryuk & Sodinokibi Spread. 2019.

Target 2

1. All three DCH Health System **hospitals** in Alabama were **temporarily closed to new patients** following a targeted ransomware attack.[6]
2. The Cancer Center of Hawaii **temporarily suspended cancer radiation treatments** at two centers due to a ransomware attack.[7]
3. Wood Ranch Medical **went out of business** after a ransomware attack caused the health provider to lose all access to their patients' medical records.[8]
4. Campbell County Health **suspended new inpatient admissions** and **canceled some surgeries** following a ransomware attack.[9]

6. Becker's Health IT & CIO Report. 3 Alabama hospitals halt admissions after ransomware attack. October 2019..
7. Becker's Health IT & CIO Report. Cancer radiation treatment halted after ransomware attack at Hawaii center. December 2019.
8. Wood Ranch Medical. Wood Rand Medical Notifies Patients of Ransomware Attack. September 2019.
9. Campbell County Health. Service Disruptions At CCH: No ETA. September 2019.

Target 2

5. Seneca Nation Health System as well as Olean Medical Group **lost access** to their **computer and EHR systems** following a ransomware attack on both of the healthcare organizations.[10]
6. Brookside ENT & Hearing Services in Michigan **closed the medical practice** after a successful ransomware attack deleted every medical record, bill, and appointment, including the backups.[11]
7. University of Arkansas for Medical Sciences **shut down its information network** after detecting a "malware virus."[12]
8. Hammersmith Medicines Research rebuffed a ransomware attack in real time, but the threat actors managed to **swipe and publish patient records online**.[13]

10. Becker's Health IT & CIO Report. 2 New York healthcare providers lose EHR access following ransomware attacks. June 2019.
11. StarTribune. All records erased, doctor's office closes after ransomware attack. April 2019.
12. Arkansas Democrat Gazette. UAMS Shuts Down Information Network After 'Malware Virus' Detected. April 2020.
13. Forbes. COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online. March 2020.

3

Technology providers, vendors, and third-party suppliers

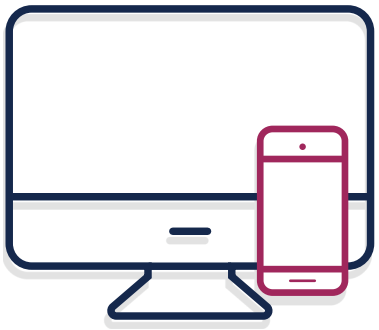
Weak security of third-party vendors in the supply chain was revealed as a new threat vector after cybercriminals breached Target through one of their refrigeration contractors. Unfortunately, healthcare organizations are not immune to supply chain attacks. Such attacks happen against medical centers through unsecured medical technology applications, vendors, and other suppliers.

In some cases, threat actors target third parties as a means to an end, looking for a less secure, easier entry into healthcare networks. For example, cybercriminals might first compromise a third-party and lay dormant on their network, pouncing at the first opportunity to grab login credentials to the healthcare network.

Target 3

In well-coordinated attacks, criminals lodge social engineering attacks against healthcare personnel pretending to be an authorized vendor with the intent to redirect huge sums of money from vendor accounts to their own.

On the other hand, cybercriminals also target vendors directly, knowing that they, too, store patient information. This is especially true of medtech companies that provide medical management apps that patients download on their mobile devices or access on their home computers. While the security of medical management apps is managed by third parties, the apps must interface and communicate with the overall security infrastructure of their associated healthcare organization. In addition, the presence of advertising or analytics trackers increases processing time, which could increase the app's vulnerability to breach.



Target 3

Impact of vendor compromise on healthcare

In scenarios where healthcare technology providers, vendors, and third-party suppliers are breached for patient data, the healthcare organizations, themselves, are not liable to pay any post-breach costs. Sadly, the result is still the theft and sale of data about patients in underground markets in the dark web with the risk of identity theft and account takeovers becoming high.

In addition, medical organizations, already on tight budgets, might need to come up with additional funds to pay the real vendors if criminals stole from vendor accounts. Finally, patients connecting to compromised medical technology platforms from home can endanger their home networks and infect additional devices.

Broad attack surface

4

The infrastructure of network-connected devices inside healthcare organizations is incredibly complex. In addition to multiple users with access to patient healthcare information (PHI), healthcare organizations use a wide variety of devices in their IT ecosystems, such as central servers, desktops, mobile devices, MRI machines, radiology equipment, PACs medical imaging files, and other equipment. Often, these systems are running old operating systems and legacy software. And these devices can all connect to the same network and central databases with little knowledge of device security.

With a combination of legacy systems and new, innovative medtech systems, the healthcare sector has a unique cybersecurity challenge. Digital expansion of PHI and a variety of healthcare devices create a broad attack surface with potential gaps in security controls and processes that create opportunities for cyber criminals to target the PHI stored on these devices.

Target 4

At the heart of the issue: many of these systems were not designed with security in mind. As noted by Yarmela Pavlovic, legal expert who advises digital health and mobile health tech companies, "... there are a lot of companies grappling with legacy products and trying to implement cybersecurity controls based on more modern technology for products where those concerns were not part of the original design and development."

Impact of broad attack surface on healthcare organizations and patients

Medical IoT devices offer new ways to monitor patients and equipment while improving care, responsiveness, and lowering costs. But this broadens the attack surface with unknown security protections. Connected medical devices—from WiFi enabled infusion pumps to smart MRI machines—increase the attack surface of devices sharing information and create security concerns, including device tampering, PII risks, and potential regulatory violations.

Target 4

For example, in July 2019 it was discovered that MiniMed Insulin Pumps had a cybersecurity vulnerability that could allow a hacker to wirelessly connect to other devices within range and change the pump's settings. As a result, the FDA issued a Class 1 recall (the most serious type of recall) on several product models that had been in distribution to healthcare patients since 1999.[14]

Cybercriminals will, no doubt, continue to focus their targets on a large number of endpoints that are less secure than traditional enterprises who are comparatively more invested in security that boast the same numbers. They find it a lot easier and more lucrative at the same time.

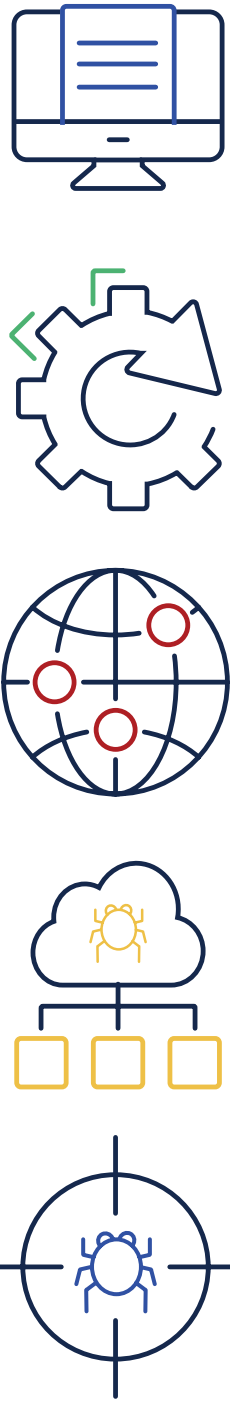
14. FDA. Medtronic Recalls Remote Controllers for MiniMed Insulin Pumps for Potential Cybersecurity Risks. 2019.

Conclusion

When it comes to making a buck out of stolen information, cybercriminals have always targeted vulnerable systems and people, whether it's local government bodies, schools, nonprofits, or individuals who are not technically savvy. Cybercriminals don't discriminate. And unfortunately, the healthcare sector remains a highly attractive target.

It is important for healthcare executive boards and IT professionals to be reminded that they have a fiduciary responsibility to ensure that patient and staff PII, including financial information, are protected; healthcare ecosystems run as normal; and operational hours are continuous. Fortunately, there are several tactics they can take to fulfill these.

Because cybercriminals have adopted a multi-vector offensive technique—a mixture of malware, social engineering, and hacking—implementing a multi-vector defensive stance to protect endpoints is the next logical step. This is done by combining good security hygiene practices and technologies that provide layered protection and detection.



Take your first step to endpoint protection

For more information about how Malwarebytes protects healthcare endpoints from malware, visit:
malwarebytes.com/healthcare