CTNT REPORT

Malwarebytes

CYBERCRIME TACTICS AND TECHNIQUES:

the 2019 state of healthcare

November 2019

Table of contents

Executive summary 3

Key takeaways 4

Global healthcare threats 5

US regional healthcare threats 11

Top attack vectors for healthcare 20

Why is healthcare a target? 22

Security challenges in healthcare 27

Consequences of a breach 32

Future concerns 33

Conclusion 36

Executive summary

> In 2019, cybercriminals stole headlines for incessant attacks against some of the world's most important sectors. Threat actors made no bones about targeting our schools to steal and sell children's data while grinding instructional hours to a halt. They gleefully tormented our cities with ransomware, putting a stop to key services and vital infrastructure. And they toyed with what some might argue is our most critical industry: healthcare.

In this special CTNT report on healthcare, we focus on the top threat categories and families that plagued the medical industry over the last year, as well as the most common attack methods used by cybercriminals to penetrate healthcare defenses. In addition, we highlight the security challenges inherent to organizations, from small private practices to enterprise health maintenance organizations (HMOs), as well as the reasons why hackers look to infiltrate their defenses. Finally, we look ahead to future biotech innovations and the need to consider security in their design and implementation.

Disruptions to healthcare data, operations, productivity, and efficiency result in severe, life-threatening consequences. Yet cybercriminals show no signs of remorse. In fact, the global data Malwarebytes Labs collected from our product telemetry, honeypots, threat intelligence, and reporting efforts from October 2018 through September 2019 shows they are only ramping up efforts. Therefore, we aim to educate those in healthcare IT and security to get ahead of the curve with an ounce of prevention…before they need a pound of breach remediation.

Key takeaways

- The medical sector is currently ranked as the seventh-most targeted industry according to Malwarebytes telemetry gathered from October 2018 through September 2019, however, overall malware detections in this industry are on the rise. Threat detections have increased for this vertical from about 14,000 healthcare-facing endpoint detections in Q2 2019 to more than 20,000 in Q3, a growth rate of 45 percent.

- The healthcare industry is overwhelmingly targeted by Trojan malware, which increased by 82 percent in Q3 2019 over the previous quarter. The two most dangerous Trojans of 2018–2019 for all industries—Emotet and TrickBot—were mostly responsible. While Emotet detections surged at the beginning of 2019, TrickBot took over in the second half as the number one threat to healthcare today.

- While we captured mostly Emotet, TrickBot, exploit, and backdoor detections targeting healthcare organizations, each of these threats are known to drop ransomware payloads later in their attack chain. Therefore, in combination with intelligence gathered and news reports on high-profile hospital ransomware attacks, we can safely conclude that ransomware is looking to penetrate healthcare organizations from several different angles.

- Of the four regions of the United States, the West's healthcare institutions were most targeted by malware, leading the pack at 42 percent of Malwarebytes' total US detections. The Midwest was not far behind, at 36 percent. However, the South and Northeast had far fewer detection percentages, at 15 and 7 percent respectively.

- The top attack methods for cybercriminals looking to penetrate healthcare networks in the last year were to compromise vulnerabilities in third-party vendor software, to take advantage of negligence or otherwise weak security postures by exploiting known vulnerabilities that haven't been patched for, and to use social engineering tactics such as phishing and spear phishing to deliver malicious emails, attachments, and links.

- The healthcare industry is a target for cybercriminals for several reasons, including their large databases of patients' personally identifiable information, lack of sophisticated security model, and high number of endpoints and other devices connected to the network. In addition, the sensitive nature of patient data that threat actors can easily swoop up lends itself to a high return on investment, which positions healthcare as a juicy target for opportunistic criminals.

- Medical institutions are fighting an uphill security battle, as budget dollars are often diverted to research, patient care, or new technology adoption. Cybersecurity, then, is an afterthought, as doctors use legacy hardware and software, staff lack the security know-how to implement updates and patches in a timely manner, and many medical devices lack security software altogether.

- Consequences of a breach for the healthcare industry far outweigh any other organization, as stolen or modified patient data can put a stop to critical procedures, and devices locked out due to ransomware attack can result in halted operations—and sometimes even patient death.

- New innovations in Internet-connected biotech, including cloud-based biometrics, Internet of Thoughts, or even advances in prosthetics represent exciting breakthroughs for healthcare, however, development and implementation without baking security into the design could result in dire outcomes. Therefore, it's important for biotech innovators to consider security in the foundation of the devices, platforms, and services themselves.

Global healthcare threats

> Statistically speaking, we can identify how much trouble the medical industry is in by examining telemetry from our business products deployed on healthcare-facing endpoints throughout the world. According to data collected from October 1, 2018 through September 30, 2019, medical organizations had fewer infections than the educational, manufacturing, and retail industries, ranking lower among the top 10 targeted sectors. That trend, however, is changing.

Comparing all of 2018 against three quarters of 2019, Malwarebytes has observed an overall 60 percent increase of threat detections from healthcare organizations. If the trend continues, we expect to see even higher gains in a full year-over-year analysis. This increase of detections is due to notorious threat families, such as TrickBot and Emotet, as well as a slew of backdoors and exploits. These tools have been custom-built and evolved into terrible machines for mass infection of organizational networks, be it huge hospital or small local practice.

With that being said, we are catching this trend at the right time. Before attacks lodged against healthcare institutes grow even more in number and severity, we can spread the word and make sure these organizations are protected from some of the most disruptive threats we've seen in the wild.

How targeted is the medical industry?

Healthcare represents a significant slice of the organizational pie, especially when considering the sheer number of brick-and-mortar medical practice locations throughout the world. This industry ranks as the seventh-most malware-focused business vertical over the last year.

Education and manufacturing took our top two spots for highest volume of threats detected in the last year. Education has been a huge target due to the large number of endpoints that are accessed on a regular basis by students, staff, and others on campus combined with outdated security infrastructure and limited staff and awareness. This creates a security nightmare that leaves many education networks full of adware, Trojans, and ransomware.

Top industries by detection

1	Education	6	Government
2	Manufacturing	**7**	**Medical**
3	Services	8	Technology
4	Retail	9	Marketing
5	Other	10	Transportation

Figure 1. Medical ranked as the 7th-most targeted industry by cybercriminals.

Manufacturing has also become a big target for attackers, as disruption of operations is almost as valuable to an attacker as being able to ransom important data. While other organizations may be able to recover from a cyberattack without losing much profit, manufacturing organizations can't afford to have their technology locked out, as it guarantees profit loss.

Yet, with an uptick in threat detections through the third quarter of 2019, we expect to see the medical industry climb this list into the next year.

Threat categories

At a high level, we like to get a general overview of the state of an industry by looking at categories of malware and other threats targeting organizations. In doing so, we're able to get a good look at the ebb and flow of malware trends over the last year, and identify where to "dig in" to find the most intrusive malware.

Figure 2 charts detections of malware categories in each quarter from the beginning of 2018 to now, with

Malware category	2018 Q1	2018 Q2	%Chg	2018 Q3	%Chg	2018 Q4	%Chg	2019 Q1	%Chg	2019 Q2	%Chg	2018 Q3	%Chg
Trojan	227	5325	2246%	6123	15%	5937	-3%	15959	169%	6652	-58%	12081	82%
Adware	96	758	690%	1297	71%	3088	138%	1561	-49%	1358	-13%	1816	34%
Backdoor	25	342	1268%	3497	923%	713	-80%	2901	307%	717	-75%	11	-98%
Ransom	4	26	550%	252	869%	150	-40%	241	61%	2158	795%	2480	15%
Malware	0	0	0%	0	0%	0	0%	500	0%	2060	312%	2206	7%
Hijack	456	457	0%	1076	135%	666	-38%	660	-1%	334	-49%	661	98%
Spyware	23	150	552%	2101	1301%	721	-66%	340	-53%	138	-59%	78	-43%
RiskWare	53	122	130%	271	122%	847	213%	591	-30%	409	-31%	757	85%
Rootkit	23	80	248%	101	26%	145	44%	170	17%	55	-68%	83	51%
Hacktool	13	21	62%	12	-43	181	1480%	98	-46%	107	9%	154	44%

	2018 Q1	2018 Q2	COMP	2018 Q3	COMP	2018 Q4	COMP	2019 Q1	COMP	2019 Q2	COMP	2018 Q3	COMP
Totals	929	7336	**690%**	14965	**104%**	11727	**-22%**	23154	**97%**	14073	**-39%**	20387	**45%**

Figure 2. Top categories of malware quarter-by-quarter, Q1 2018 – Q3 2019

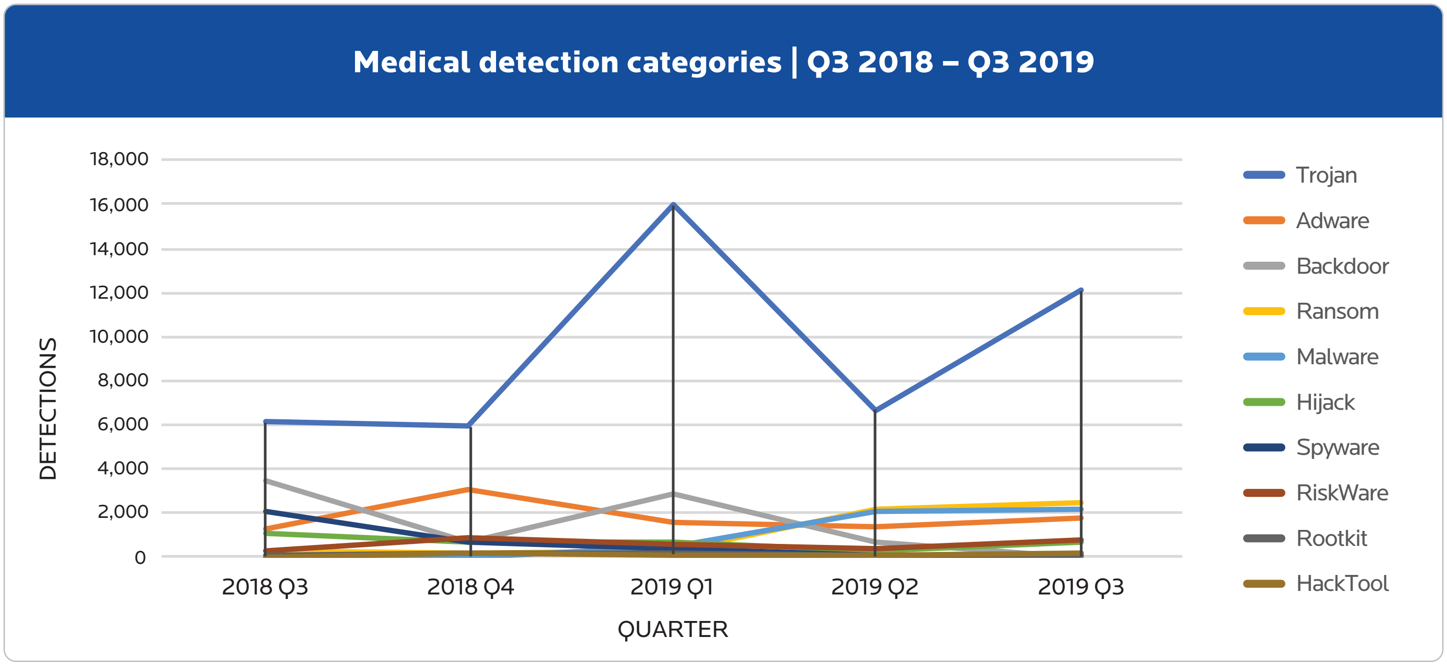


Figure 3. Malware category detections, healthcare

quarter-over-quarter percentage changes tracked between quarters. For example, you can see that in Q3 2019, all threat categories increased by 45 percent over the previous quarter. In fact, the only categories of threats that saw declining numbers were backdoors and spyware. Trojans, hijackers, and riskware in particular each surged ahead by over 80 percent from Q2 2019.

Figure 3 expresses the same data but in visual form, showing us how much greater the number of detections for Trojan malware is than for any other category.

However, since Trojan is such a broad category of malware, encompassing anything from downloaders to botnet clients, it helps to identify which threat families are responsible for the uptick. That's when we drill down another level.

Threat families

Looking at the overwhelming number of Trojans targeting the healthcare industry, we can dig into which caused the most problems for the medical industry by examining the top 10 threat families, Trojan or otherwise, that the medical industry has been fighting since October 2018.

Figure 4 expresses the activity of the top 10 threat families against medical organizations, according to our detections over the last year. Here you can see why we see so much Trojan malware—massive spikes of Emotet, which we classify as a Trojan, occurred in late 2019 and throughout Q1 2019. However, other Trojan families such as TrickBot kept the trend going.

Another conclusion we can draw from this graph is that ransomware is looking to step in from several angles. Not only have many hospitals failed to patch the SMB vulnerabilities that WannaCry

Top 10 medical threats | October 1, 2018 - September 30, 2019

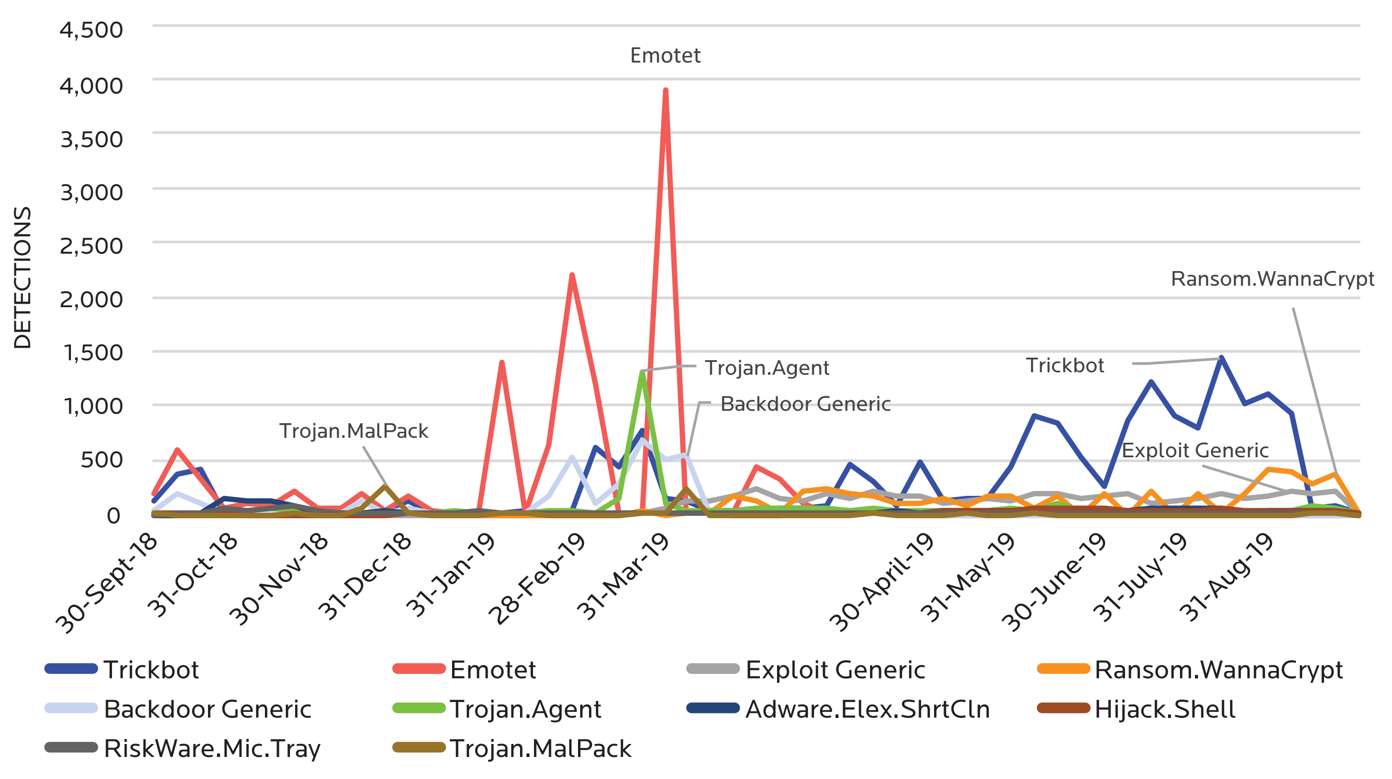


Figure 4. Top threat families targeting healthcare 2018 – 2019

used, but many of the Trojans leveraged against healthcare are also known to deliver ransomware payloads. For example, Emotet not only launches TrickBot as a secondary payload, but both Emotet and TrickBot often drop Ryuk ransomware in a combination attack we've come to call "the triple threat." Ransomware payloads are also common deliverables of exploits, which we've detected aimed at healthcare since early 2019. Therefore, where Malwarebytes detection and remediation reports show us Trojans, we would expect to encounter ransomware later in the infection process if the threats were allowed to fester on.

Stripping away some of the less important detections, we can dig deeper into what is happening with Emotet, TrickBot, and a couple of their "friends."

Figure 5 allows a clear look at trend activity with these families over the last year. We chose to focus on these four families not only because of their detection amounts, but also because of their potential damage and/or part in the distribution of other threats.

Emotet strikes back

Emotet originally started out as a banking Trojan, but has developed into a versatile harvesting and infection tool. It is a modular software package that can be easily adapted to perform several malicious tasks. One of those modules is a highly-effective spam tool that has a higher infection rate than similar malware because of its ability to spoof senders that are known to the victim. It can even hijack existing email conversations. Last year, the US Department of

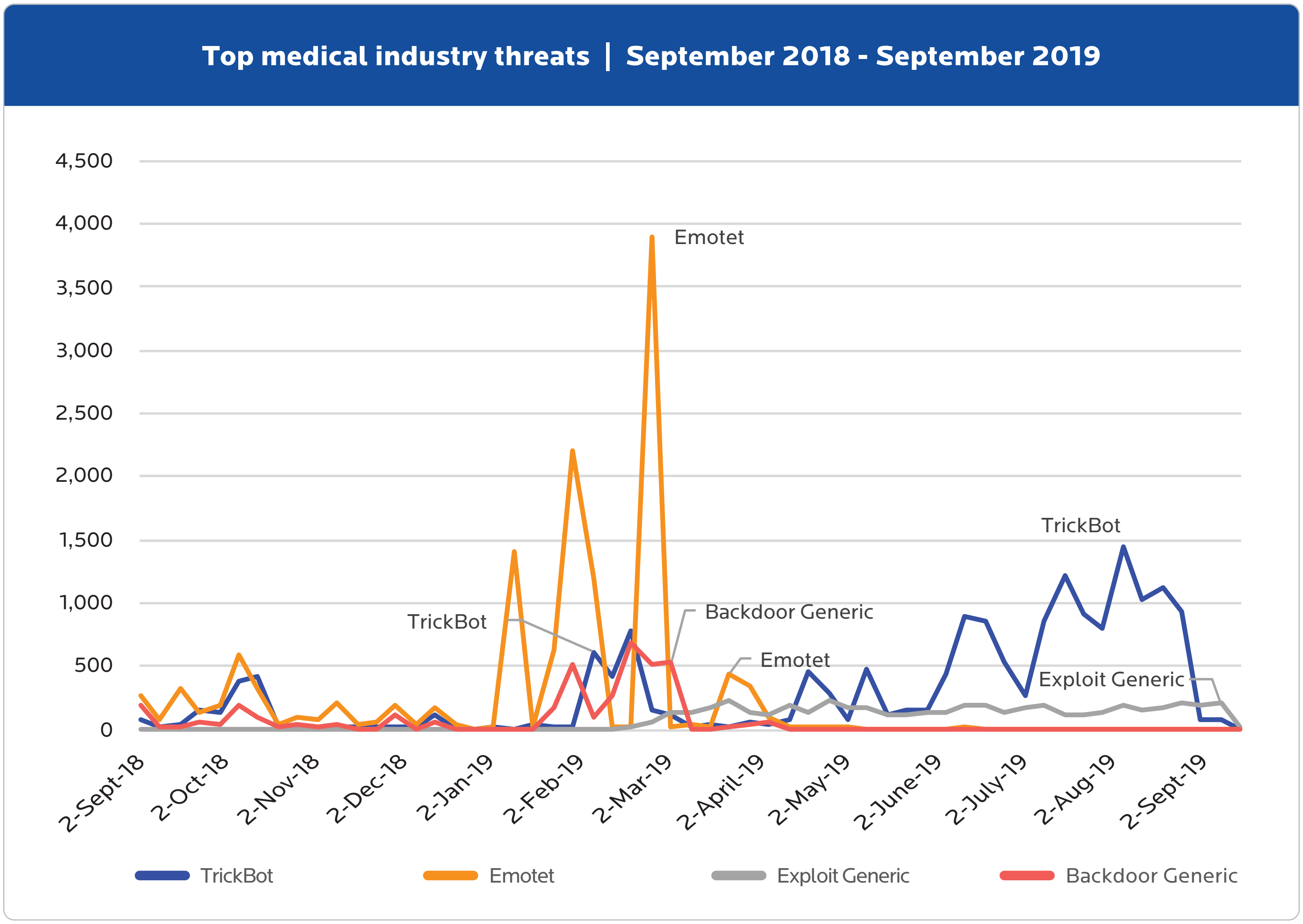


Figure 5. Most dangerous threat families targeting healthcare

Homeland Security deemed Emotet the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments.

During Q1 2019, Emotet was running wild in the medical industry. However, much like Emotet's distribution pattern across the world and in other industries, by the time summer rolled around, it had gone offline. As of this writing, Emotet has come back; however we'll have to wait until later in the year before we can see how this new campaign impacts healthcare.

Another interesting observation is the higher detection of generic backdoors in February and March, which are used to get around typical security measures and gain access into healthcare networks. This coincides somewhat with the spikes of Emotet, and falls off the map just as quickly as Emotet does by April, indicating the backdoors could have been used to drop Emotet on healthcare networks. It's around this time that we start to see a bigger shift. While Emotet is absent, TrickBot fills in the gap with a slow and steady push over the mid to late summer.

From March 2019 onward, we observed a low-laying, consistent dribble of exploit activity accompanying TrickBot detections. This tracks with what we know about common TrickBot (and Emotet) infection methods, which include the use of malicious scripts launched from Microsoft Office documents, zipped files, or drive-by exploit links.

TrickBot or treat!

TrickBot is a notorious Trojan malware that has been terrorizing organizations for more than a year. Over the last 12 months, we've observed this threat evolve from a simple malware that steals bank information to a full-fledged network infection monster. TrickBot's

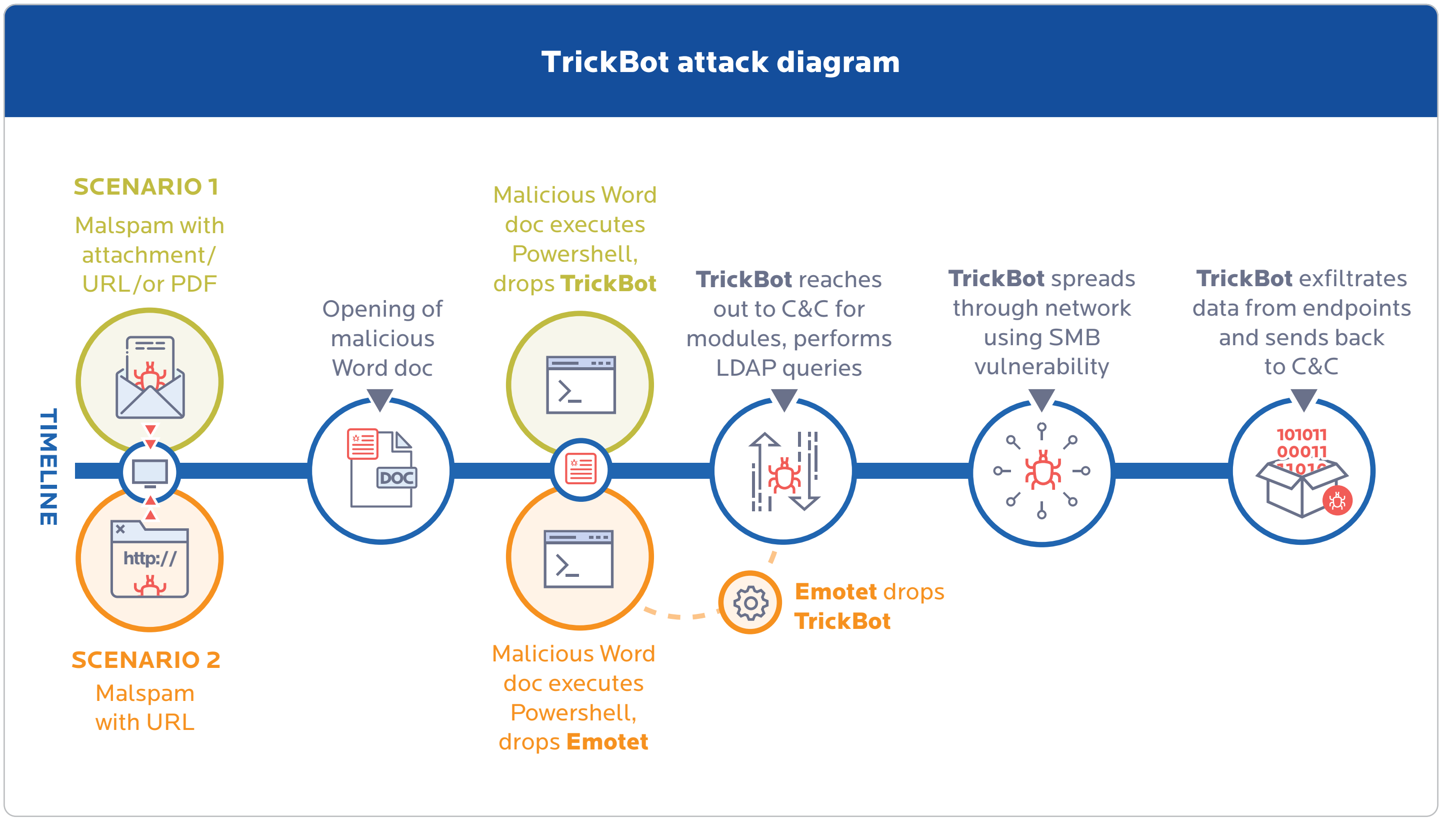

TrickBot attack diagram
SCENARIO 1
Malspam with attachment/ URL/or PDF
TIMELINE
http://
SCENARIO 2
Malspam with URL
Opening of malicious Word doc
DOC
Malicious Word doc executes Powershell, drops TrickBot
Malicious Word doc executes Powershell, drops Emotet
TrickBot reaches out to C&C for modules, performs LDAP queries
Emotet drops TrickBot
TrickBot spreads through network using SMB vulnerability
TrickBot exfiltrates data from endpoints and sends back to C&C
101011
00011
1010

Figure 6. Diagram of TrickBot/Emotet infection vector with exploit.

latest tricks include being able to brute-force credentials and launch exploits to achieve lateral movement. A new feature that has been reported is the ability to launch SIM swapping attacks, a method to get around SMS-based authentication means. TrickBot spent the second half of 2018 heavily targeting services, education, and manufacturing, as you can see in Figure 7.

Depending on the time of year, general services, manufacturing, retail, and education were all bigger targets for TrickBot than healthcare. However, by the beginning of June, you can see that all other industry detections dropped off, while the only one on the rise was medical. Does this mean that TrickBot is going to be a massive thorn in the side of the medical industry for quarters to come? Anything is possible when it comes to cybercrime and malware, especially now that Emotet has made a splashy return to the scene. Only time will tell which industry TrickBot might ensnare next.

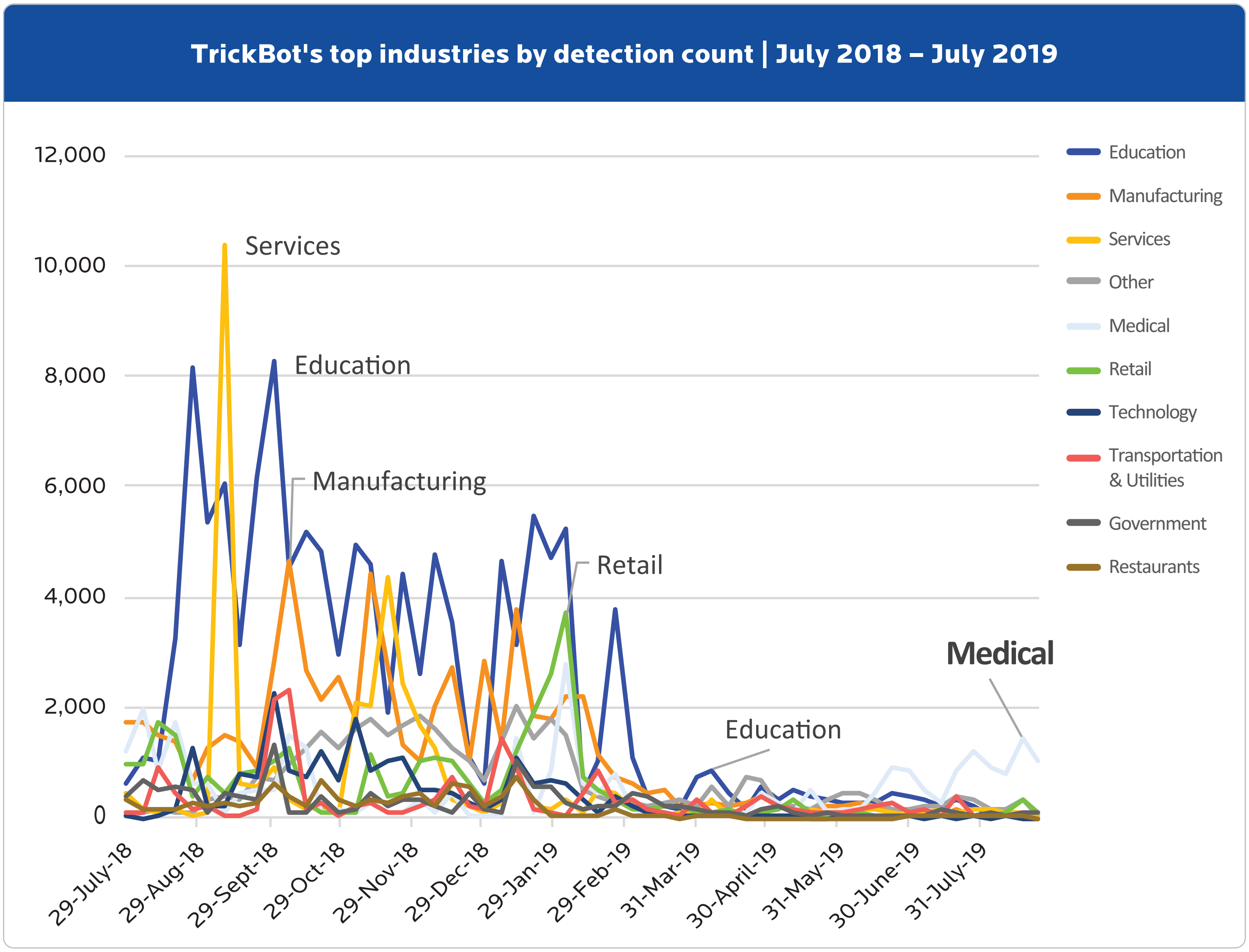


Figure 7. TrickBot industry targets, July 2018 – July 2019

US regional healthcare threats

> To identify unique circumstances and trends associated with healthcare-focused threats in specific geographic areas, we sliced up detections in the United States (which represents a large percentage of our medical customers) into four regions. These regions, as defined by the US government Census Bureau, are the Northeast, South, Midwest, and West.

Top regions targeted by cyberthreats

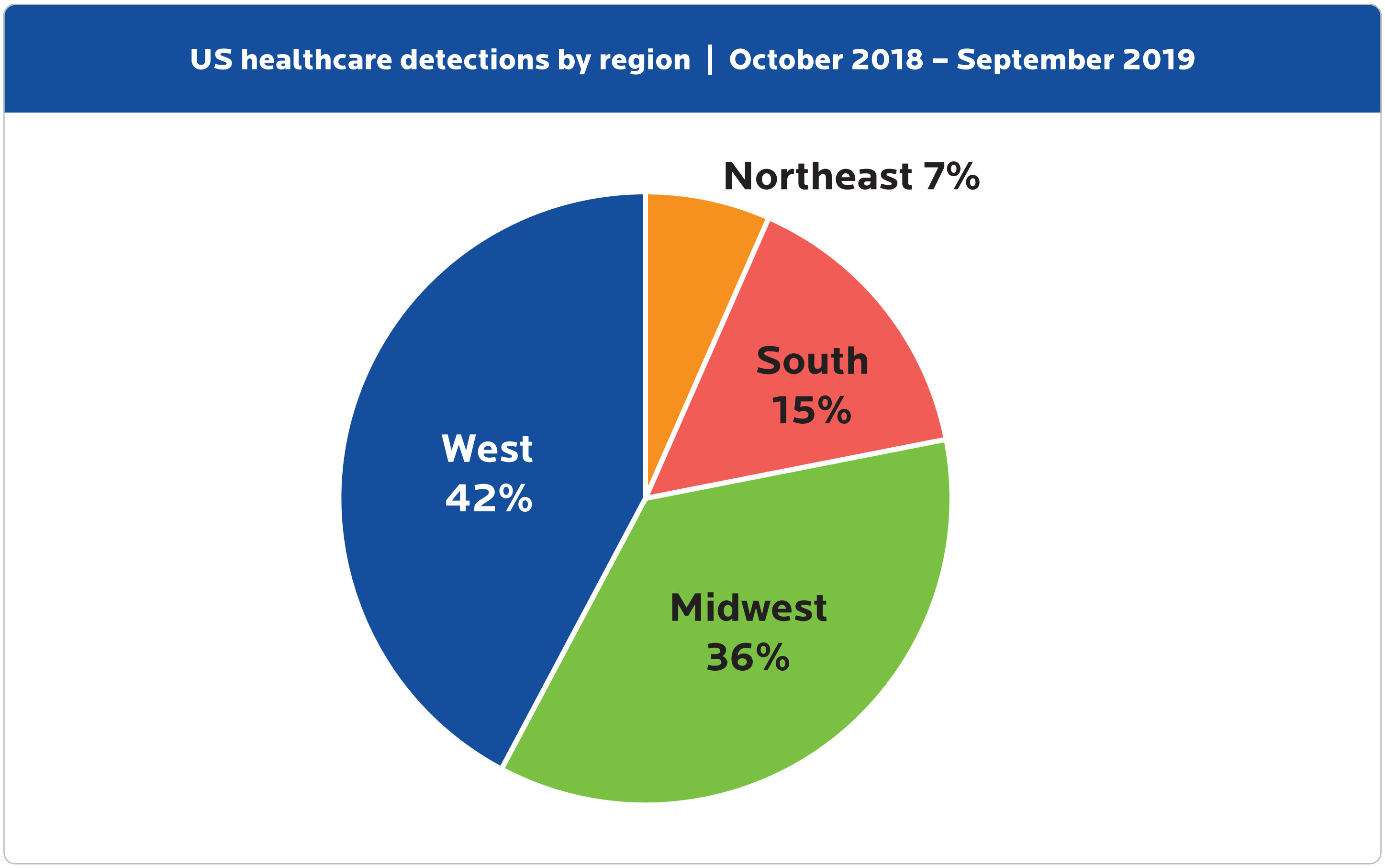


Figure 8. Percentage of healthcare threats per region

We began by looking at overall malware detections between the four regions. The West region had the highest number, with nearly 24,000 threat detections over the last year, or 42 percent of total US healthcare detections. The Midwest wasn't far behind with 36 percent of US healthcare detections.

The South and Northeast, however, had fewer medical-focused malware attacks than their western peers by a significant amount. For example, the Northeast only registered 3,655 detections—at least 20,000 fewer than the West.

West

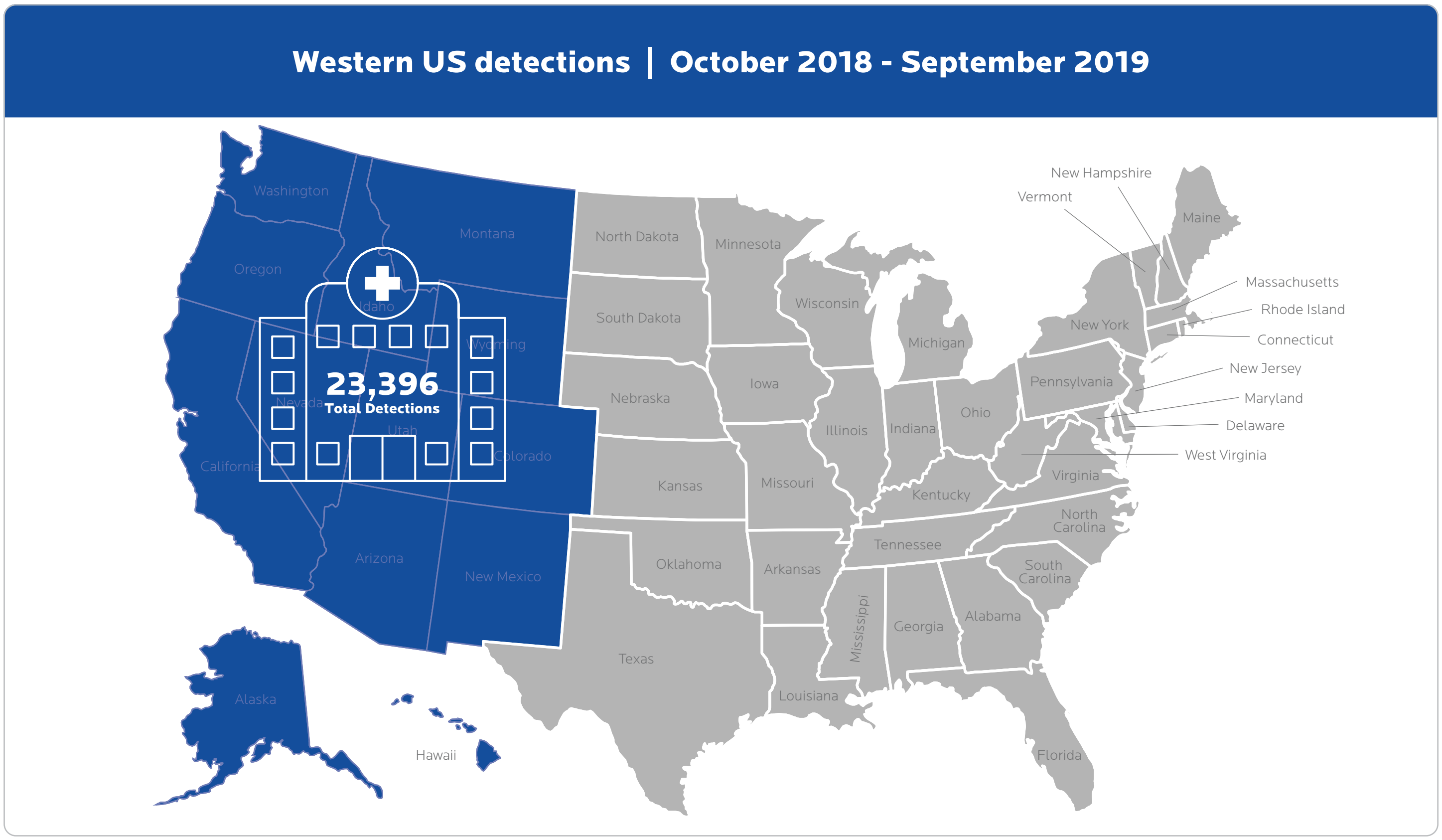


Figure 9. The West had the highest number and percentage of threats aimed at US health organizations.

From October 2018 through September 2019, the West region experienced 23,396 total detections of threats aimed at the medical industry. This region includes the 11 contiguous states of Washington, Oregon, California, Idaho, Nevada, Arizona, Utah, Montana, Wyoming, Colorado, and New Mexico, as well as Hawaii and Alaska. Of these, the top five states targeted were Idaho, California, New Mexico, Nevada, and Colorado.

Threat category	Threat family
1. Trojans	Emotet
2. Backdoors	Generic backdoors
3. Adware	TrickBot
4. Generic malware	Generic exploits
5. Hijackers	Hijack.SecurityRun

Figure 10. Top Western threat categories and families

The top five categories and families of healthcare threat detections in the West were:

- From February to March 2019, medical organizations in Montpelier and Preston, Idaho, dealt with heavy detections of Emotet.
- From December 2018 to mid-February 2019, there was a heavy active TrickBot campaign.

Midwest

Midwestern US detections | October 2018 - September 2019

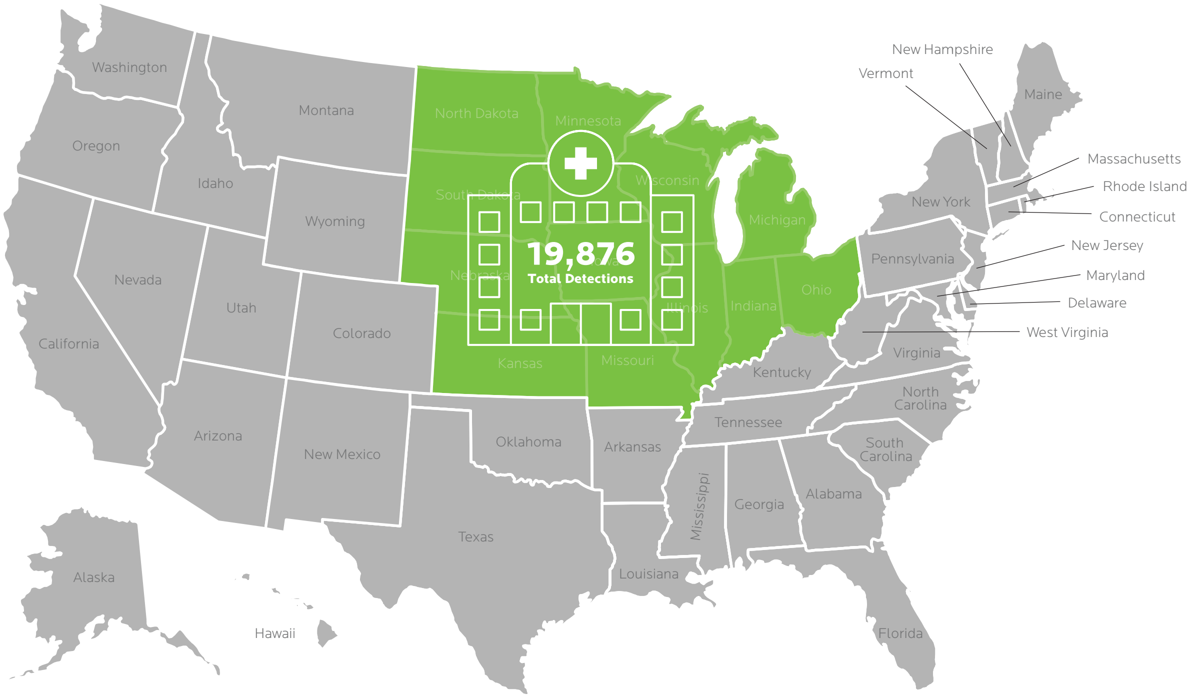


Figure 11. The Midwest included the highest number and percentage of US healthcare threats.

During our research period, the second-most targeted US region was the Midwest, with 19,876 detections in the healthcare vertical, and 36 percent of total US detections. The Midwest region features 12 states: North Dakota, South Dakota, Kansas, Nebraska, Minnesota, Wisconsin, Michigan, Illinois, Iowa, Ohio, Missouri, and Indiana. Of these, the top five states targeted were Illinois, Ohio, Wisconsin, Michigan, and Kansas.

Threat category	Threat family
1. Trojans	Emotet
2. Backdoors	Generic backdoors
3. Adware	TrickBot
4. Generic malware	Generic exploits
5. Hijackers	Hijack.SecurityRun

Figure 12. Top Midwestern threat categories and families

The top five categories and families of healthcare threat detections in the Midwest were:

- Medical organizations in Illinois dealt with a heavy blow from TrickBot from mid-April to early September 2019.
- Emotet was heavily distributed in the Midwest from December 2018 to mid-January 2019.

South

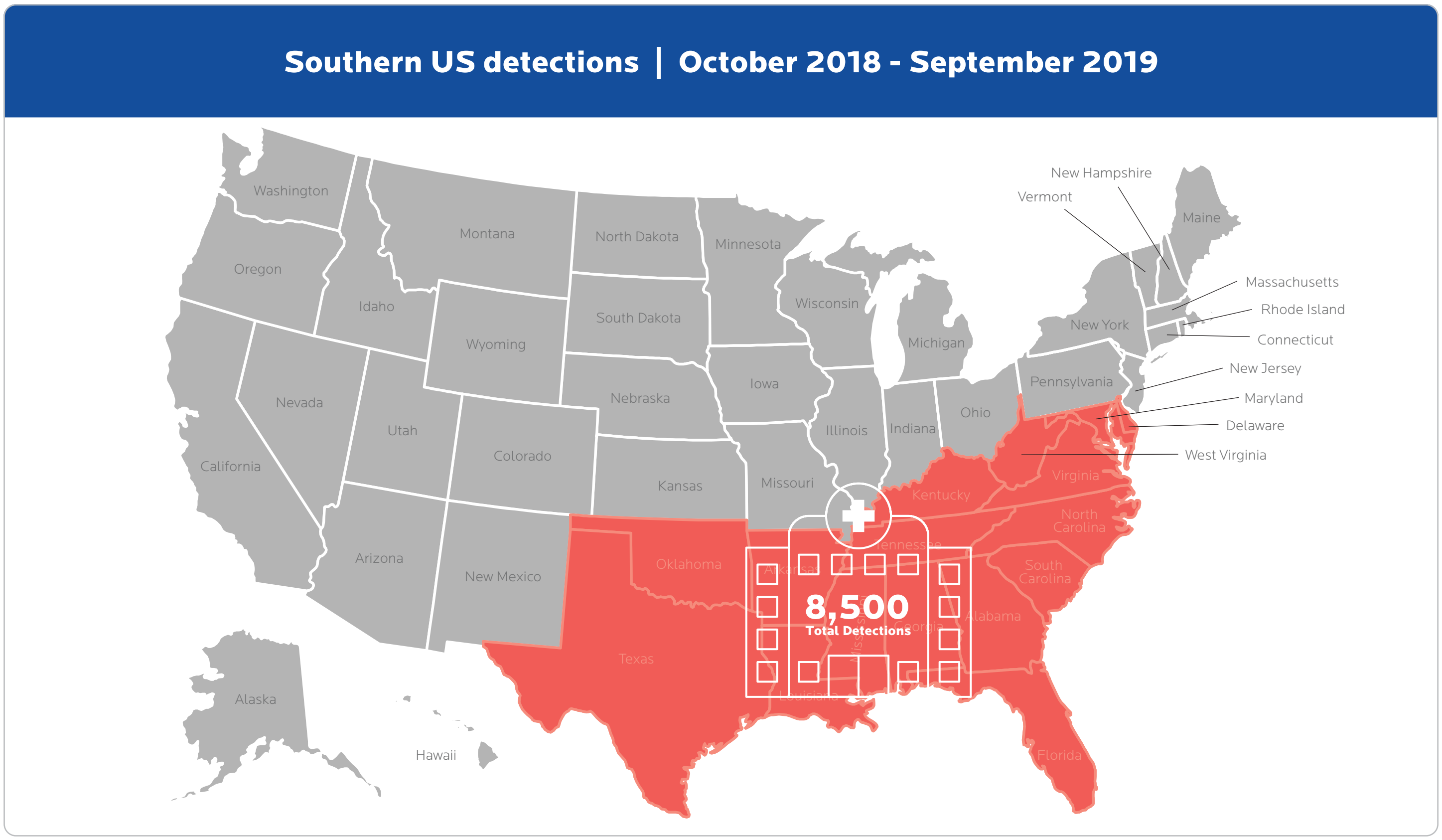

Southern US detections | October 2018 - September 2019

Figure 13. The South had only 15 percent of total US healthcare threat detections.

Third on the list of US regions is the South. Despite having the largest number of states—16 states, plus Washington, D.C.—the South contained a much smaller percentage of total detections at just under 8,500 or 15 percent. The top five most-targeted Southern states were, in order Texas, Kentucky, Florida, Virginia, and Georgia.

Threat category	Threat family
1. Trojans	Emotet
2. Backdoors	Generic backdoors
3. Adware	TrickBot
4. Generic malware	Generic exploits
5. Hijackers	Hijack.SecurityRun

Figure 14. Top Southern threat categories and families

The top five categories and families of healthcare-facing threat detections in the South may already be familiar. They include:

- January to February 2019 saw an increase in Emotet detections for this region, specifically in East Texas. We saw over twice as much Emotet during this period as any other family of malware.
- Meanwhile, Georgia dealt with heavy detections of TrickBot, along with Virginia and Texas, from April to early September.
- During April, while TrickBot was being pushed heavily, we observed a spike in detections of exploit attempts, likely associated with TrickBot's methods of spreading.

Northeast

Northeastern US detections | October 2018 - September 2019

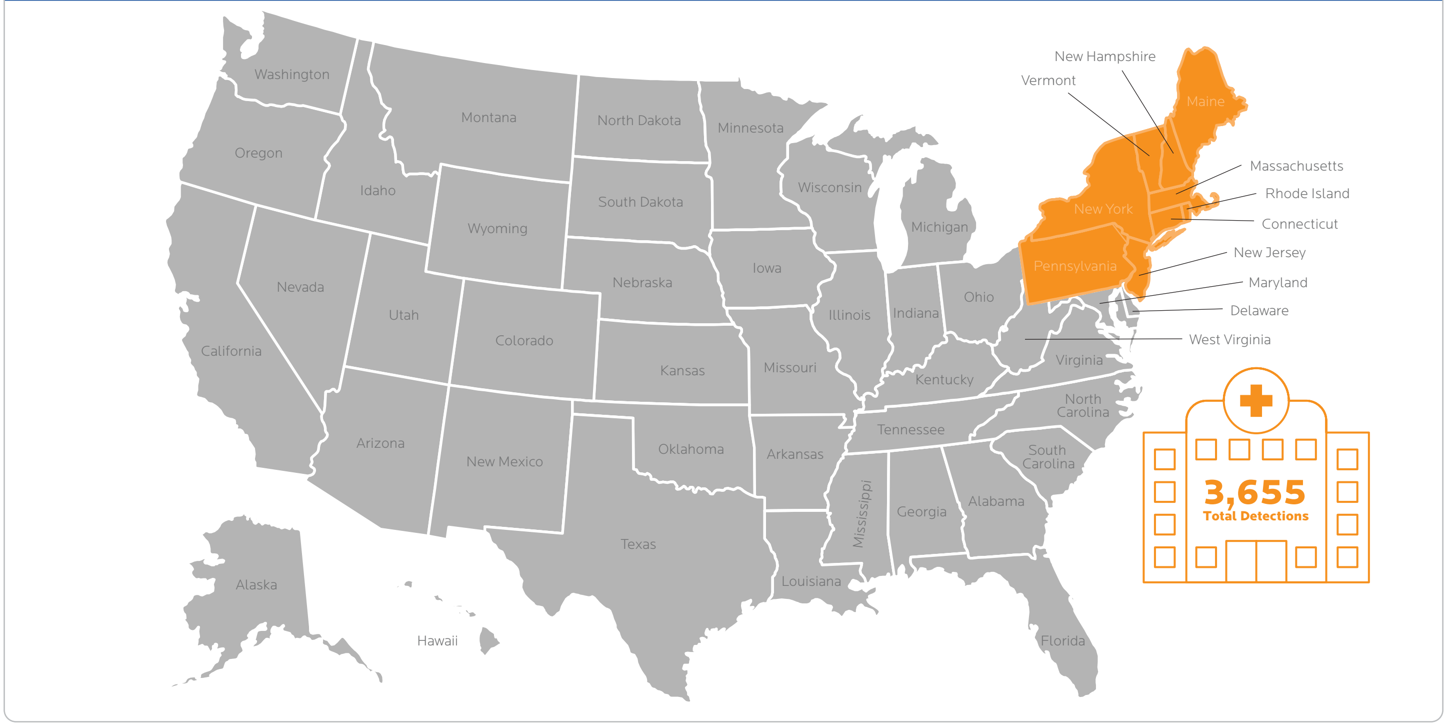


Figure 15. Only 7 percent of healthcare-focused threats were detected in the Northeast.

With just 3,655 detections of medical-facing threats, the Northeast had the smallest number of threats of all the regions. Just 7 percent of total US healthcare threats hit the states of Maine, New Hampshire, Vermont, Massachusetts, Connecticut, Rhode Island, New York, New Jersey, and Pennsylvania. From highest to lowest, the top five Northeastern states were New York, New Hampshire, Massachusetts, New Jersey, and Connecticut.

Threat category	Threat family
1. Adware	Hijack.Tray
2. Hijackers	Riskware.MicTray
3. Riskware	Emotet
4. Trojans	Generic exploits
5. Generic malware	Hijack.FolderOptions

Figure 16. Top Northeastern threat categories and families

The top five categories and families of healthcare threats detections in the Northeast paint a slightly different picture. They are:

- The biggest spike in Emotet detections in the Northeast occurred in Late March, with little activity afterward and few detections previously.
- Exploit activity spiked from mid-August to late September, primarily detections from medical organizations in Philadelphia, Pennsylvania.

Tracking healthcare campaigns

To figure out which regions experienced cyberattacks on their healthcare institutions, and at which time of the year, we drilled down through our data from a different angle, investigating and tracking each region's detections along a timeline. By viewing them this way, we hoped to be able to correlate spikes in regional detections with spikes in threat categories and families, enabling us to determine whether there was an active, geotargeted campaign or a steady stream of diverse threats spread across the country. Starting with the four regions' overall threats, we observed spikes at various times of the year for all regions but the Northeast.

According to Figure 17, the West dealt with the most malware for at the beginning of 2019, trending mostly upward until a large spike on March 3, 2019. The South shared the West's early 2019 spike, but dropped off before the highest peak in March. The Midwest, meanwhile, collected most of its detections outside of this time period, showing up near the end of our timeframe and spiking in mid-August. To better understand what caused these spikes, we compared them against the top threat categories shared by all US regions.

We noticed that both instances of regional spikes coincided with spikes of Trojan malware, so we once again examined Trojans to see which families were responsible. Doing so gave us some pretty obvious results. For clarity, we removed everything but the top offenders in the Trojan category, and you should recognize them.

Quite clearly, Emotet was responsible for the early 2019 regional spikes of detections in the South and West. And, almost as if picking up the ball once Emotet left the court, TrickBot slowly increased in detections from March until around mid-August. It's likely that Emotet authors knowingly passed the torch to TrickBot once they decided to take a break for the summer.

US regional detection trends | September 2018 – September 2019

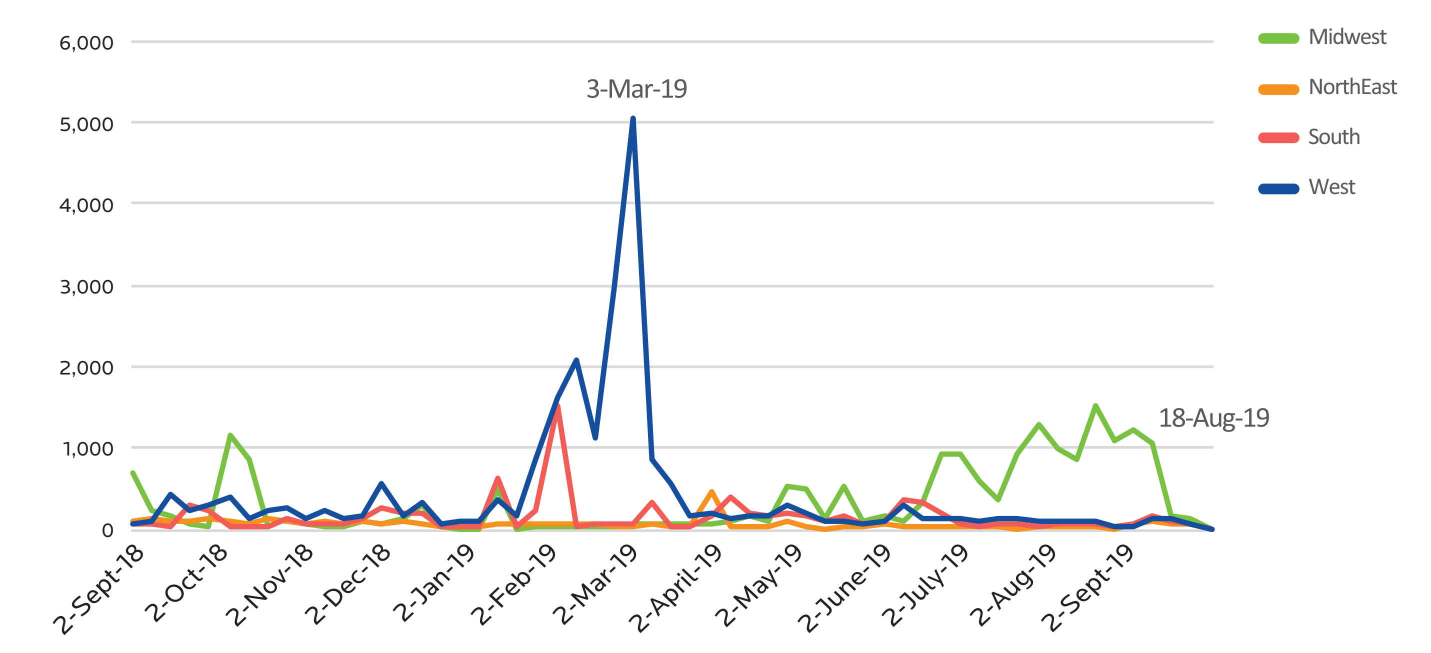


Figure 17. Regional healthcare detections timeline

Threat category by detection | United States | September 2018 - 2019

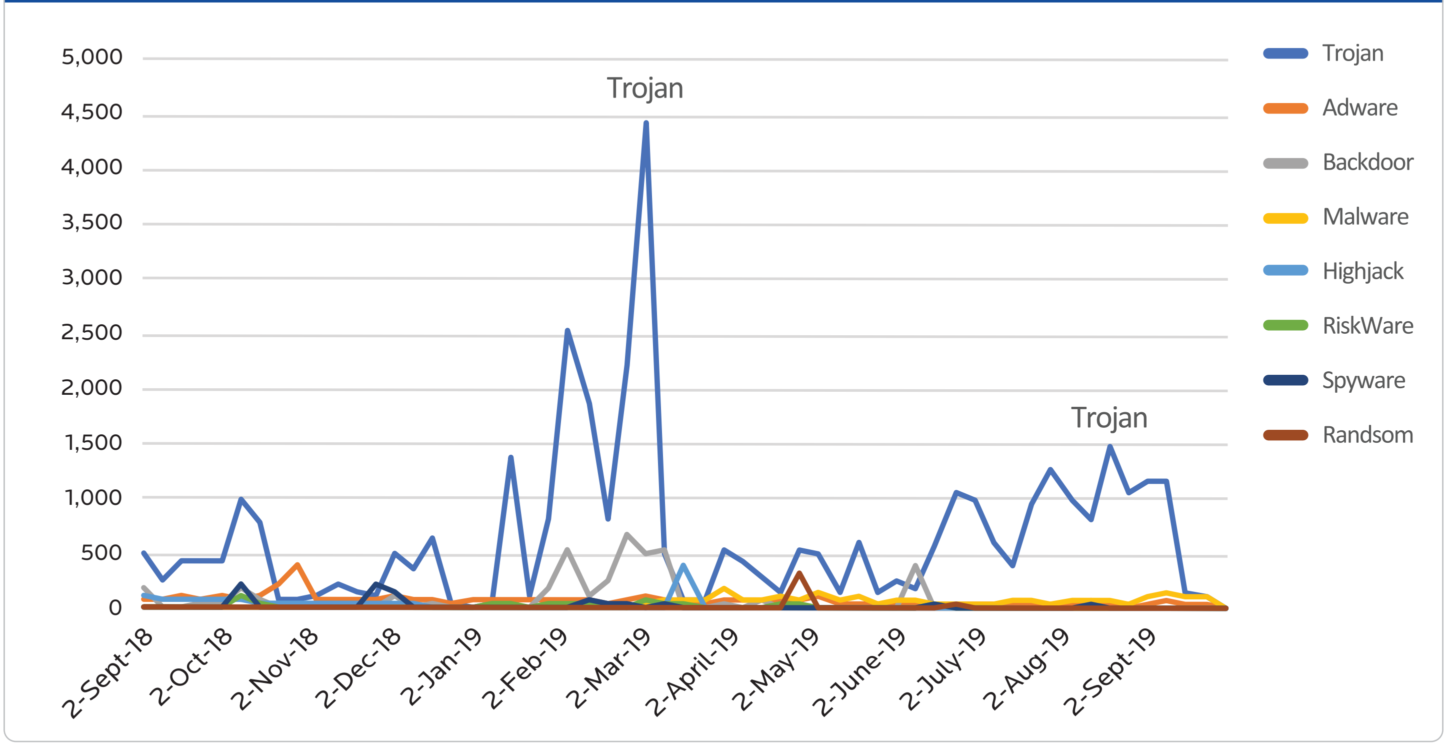


Figure 18. Spikes in the top threat categories match with regional spikes.

TrickBot and Emotet detection trends | September 2018 - 2019

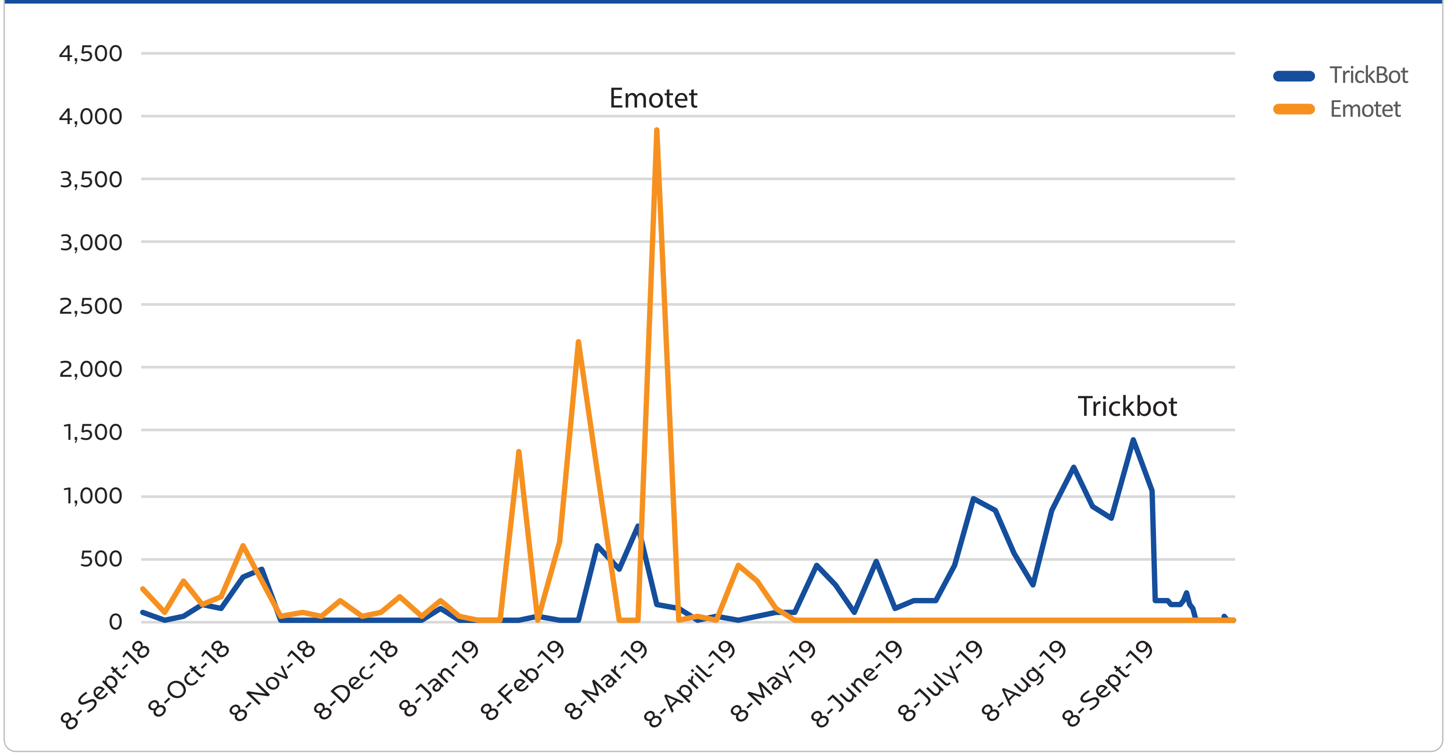


Figure 19. TrickBot and Emotet, at it again

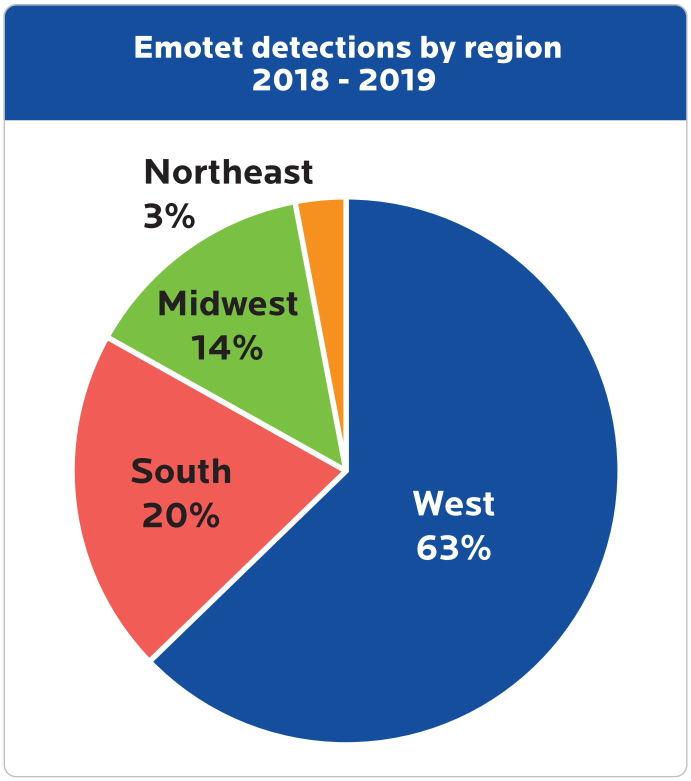


Figure 20. Emotet percentage by the regions

As far as which regions' healthcare organizations were most effected by Emotet, we created an easy-to-understand chart, with the West clearly being a huge target. In fact, the top states for Emotet detections were in the West: Idaho, Nevada, Arizona, and Wyoming.

Looking at this data from a different perspective, we can find out which regions have been most impacted by Emotet over time. According to Figure 21, the West was the most-heavily targeted region by Emotet, which we already knew, but there is something unique here we couldn't see before.

The South dealt with a heavy amount of Emotet detections (equal to what the West was fighting at the time) one month prior to the massive spike in the West. This kind of data is useful when trying to understand distribution strategies of malware authors. With a month between major pushes, versions

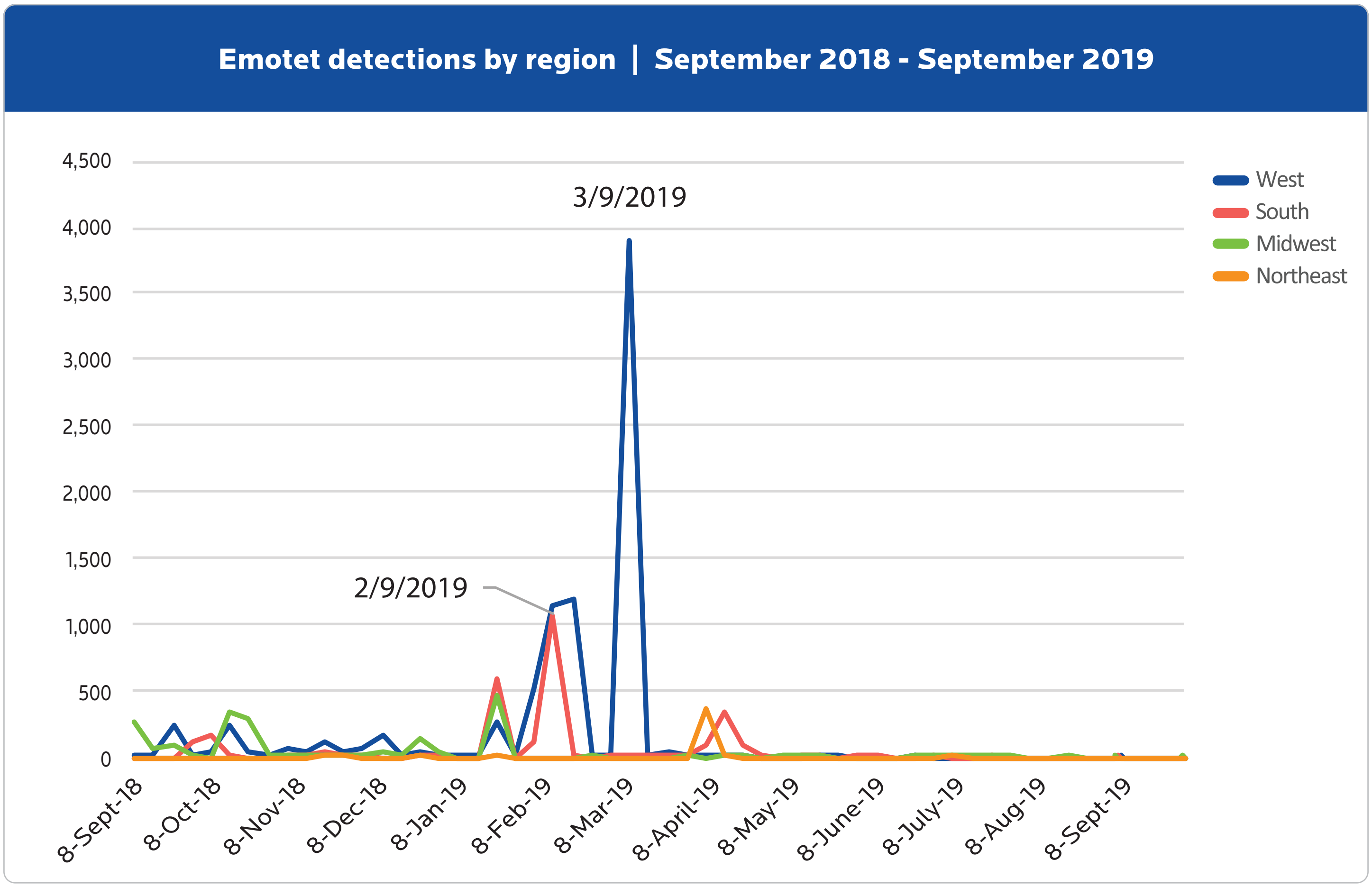


Figure 21. Emotet detections by US region

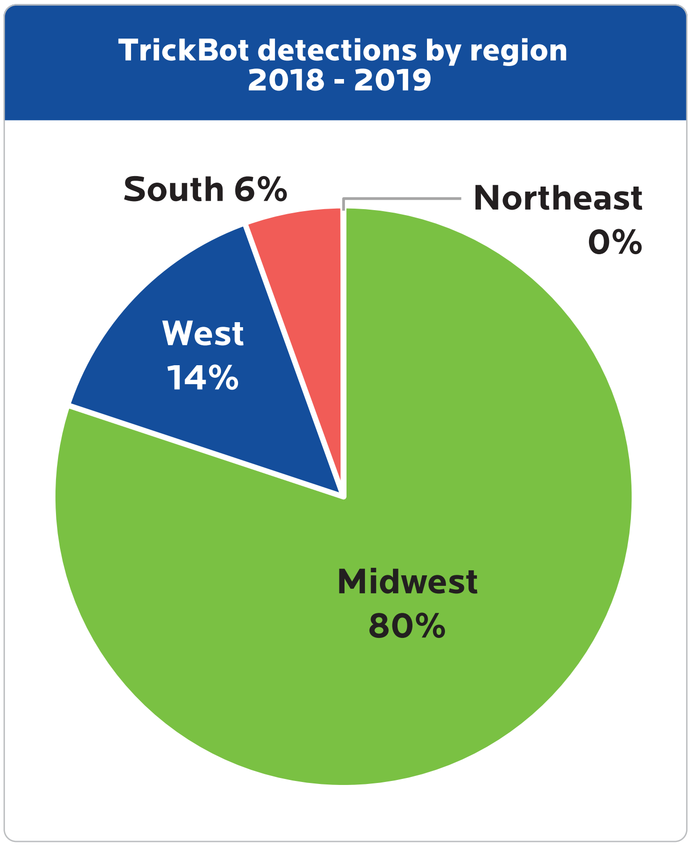


Figure 22. TrickBot percentage by the regions

of Emotet which may have been blocked during February had likely been updated to be more effective by March. Therefore, we saw such a greater spike.

We can conduct the same analysis with TrickBot. TrickBot has been a massive problem for medical organizations in the Midwest; moreso than Emotet was for the West. The top states affected by TrickBot are: Illinois, Ohio, and Michigan, specifically the cities of Chicago, Illinois, and Franklin, Ohio.

With such domination in the Midwest, you would expect to see massive spikes like Emotet in TrickBot's distribution. However, TrickBot's attack method seems to be the slow and steady approach, allowing it to fall just below the top threat, but above anything else in the region.

If we stretch out the timeframe of these detections, we can see the same lines as earlier, except without Emotet blocking the view. The Midwest was plagued with TrickBot primarily near the end of the period, from early May to late August.

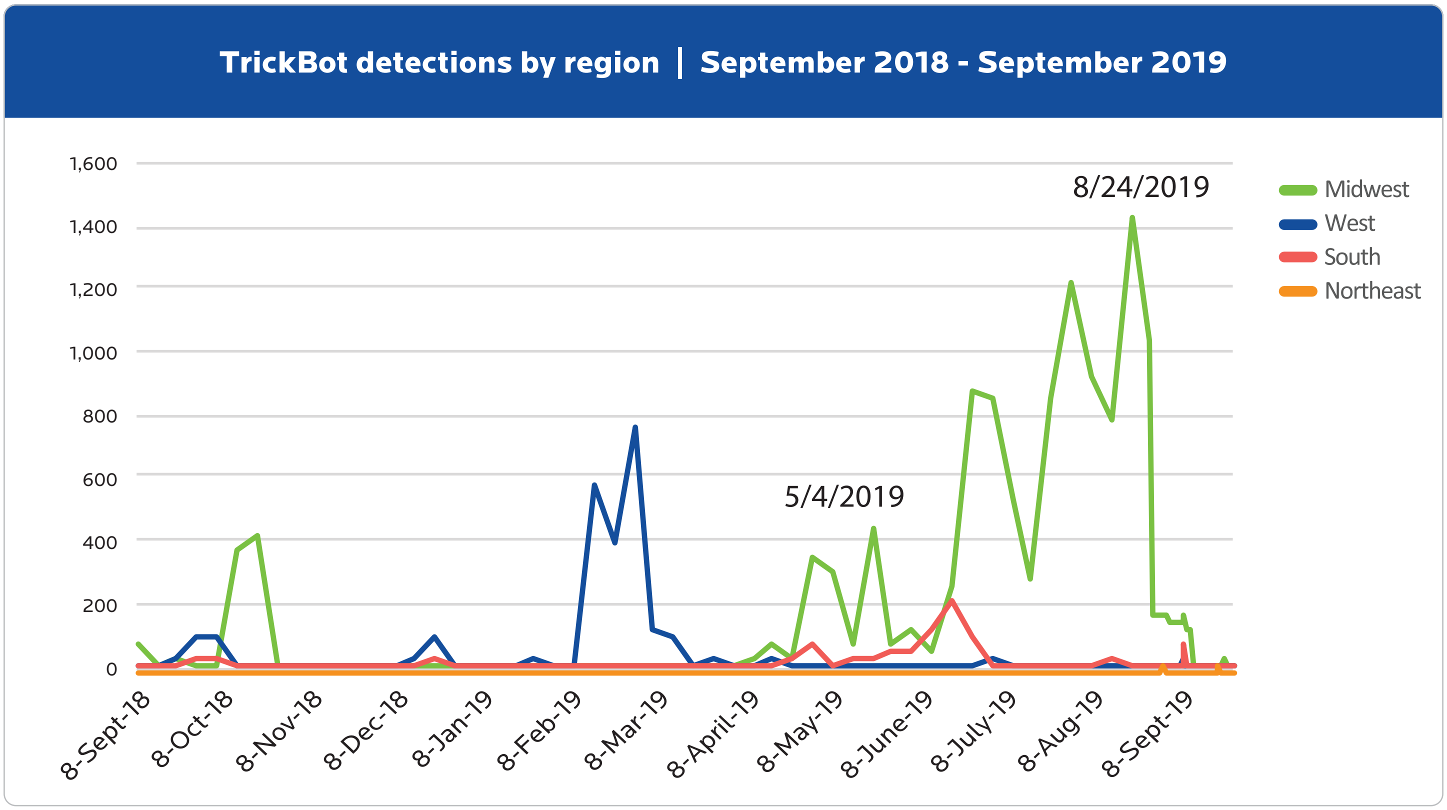


Figure 23. TrickBot dominates in the Midwest

Why Emotet and TrickBot?

Whichever way we slice global and regional data on healthcare organizations, two threats come out on top: Emotet and TrickBot. These two intrusive, sophisticated Trojans are also the primary threats to other industries with high numbers of endpoints but less advanced security models, such as education and local government agencies. Emotet and TrickBot are known to spread primarily through a combination of social engineering and abuse of misconfigured and unpatched systems and security tools.

However, TrickBot is specifically known for its ability to move laterally by stealing user credentials, exploiting unpatched vulnerabilities, and more recently, spreading spam from infected systems, something we previously watched from Emotet. It's possible that because of the many ways this threat can spread, we're seeing such a large area of infection.

Was the West targeted by Emotet and the Midwest intentionally the focus of TrickBot? Or were these just attacks of opportunity that got a foothold in these respective regions? In the next sections of the report, we examine top attack vectors and security pain points for the healthcare industry, as well as the potential profits for cybercriminals to search for the answers.

Top attack vectors for healthcare

> When cybercriminals consider how to attack an organization and reap the highest reward, they ponder the industry's known weaknesses and how best to exploit them. Three major attack vectors were responsible for the majority of healthcare-focused attacks in 2018–2019: third-party supplier vulnerabilities, negligence, and phishing.

Because healthcare providers have less sophisticated security models, more complex ecosystems, and limited cybersecurity training for staff, they represent prime opportunities for cybercriminals. And cybercriminals have wizened up. They fully understand that healthcare providers include large numbers of diverse endpoints that house critical, valuable data, surrounded by only a few guards. It wouldn't be surprising to see healthcare caught up in a wave of campaigns aimed at other organizations with less fortified defenses.

Two of the top attack vectors for cybercriminals targeting healthcare institutions are aimed squarely at exploiting vulnerabilities and other security weaknesses inherent in the medical field. Therefore, look for more information on third-party vulnerabilities and employee and administrative negligence in the *Security challenges in healthcare* section of the report. Instead, we will focus on phishing as the main attack vector for hospitals and other healthcare institutions in 2018–2019.

Phishing

As with many other organizations today, healthcare institutions often fall victim to social engineering attacks, most often phishing or spear-phishing emails. In March 2019, Brigham and Women's Hospital in Boston, Massachusetts, released a study indicating that hospital employees were extremely vulnerable to phishing attacks, with research participants clicking on 14 percent of the phishing emails they received, or one in seven. With so much email communication between healthcare organizations, patients, doctors, and other staff members taking place daily, any rate of deception is alarming. Factor in sensitive data transmitted via email or stored in networks breached via phish, and you have a recipe for breach disaster.

Phishing's business partner, the business email compromise, or BEC scam, does not involve fancy creation of malicious code or the exploitation of weaknesses in systems. It does, however, bank on healthcare staff not knowing that they are being socially engineered.

These known risk factors likely ushered a series of BEC scams in 2016 that targeted 17 healthcare institutions in the US, 10 in the UK, and eight in Canada. Further, a ProofPoint study of more than 160 billion emails sent across 150 countries in 2017 and 2018 found that the frequency of email fraud attacks targeting healthcare organizations increased by 473 percent from about two years prior.

Phishing as a top attack vector for healthcare also tracks with the top threats lodged at healthcare over the last year, TrickBot and Emotet, as they are most often delivered via phishing email. Threat actors send emails disguised as unpaid invoices or requests to update account information, and healthcare employees are tricked into opening attachments or clicking on malicious links that launch the attack.

But why phish healthcare organizations in the first place? Why bother penetrating networks and taking advantage of unpatched systems or tricking users into launching attacks? In our next section, we examine the reasons why cybercriminals have been ramping up attacks on healthcare organizations.

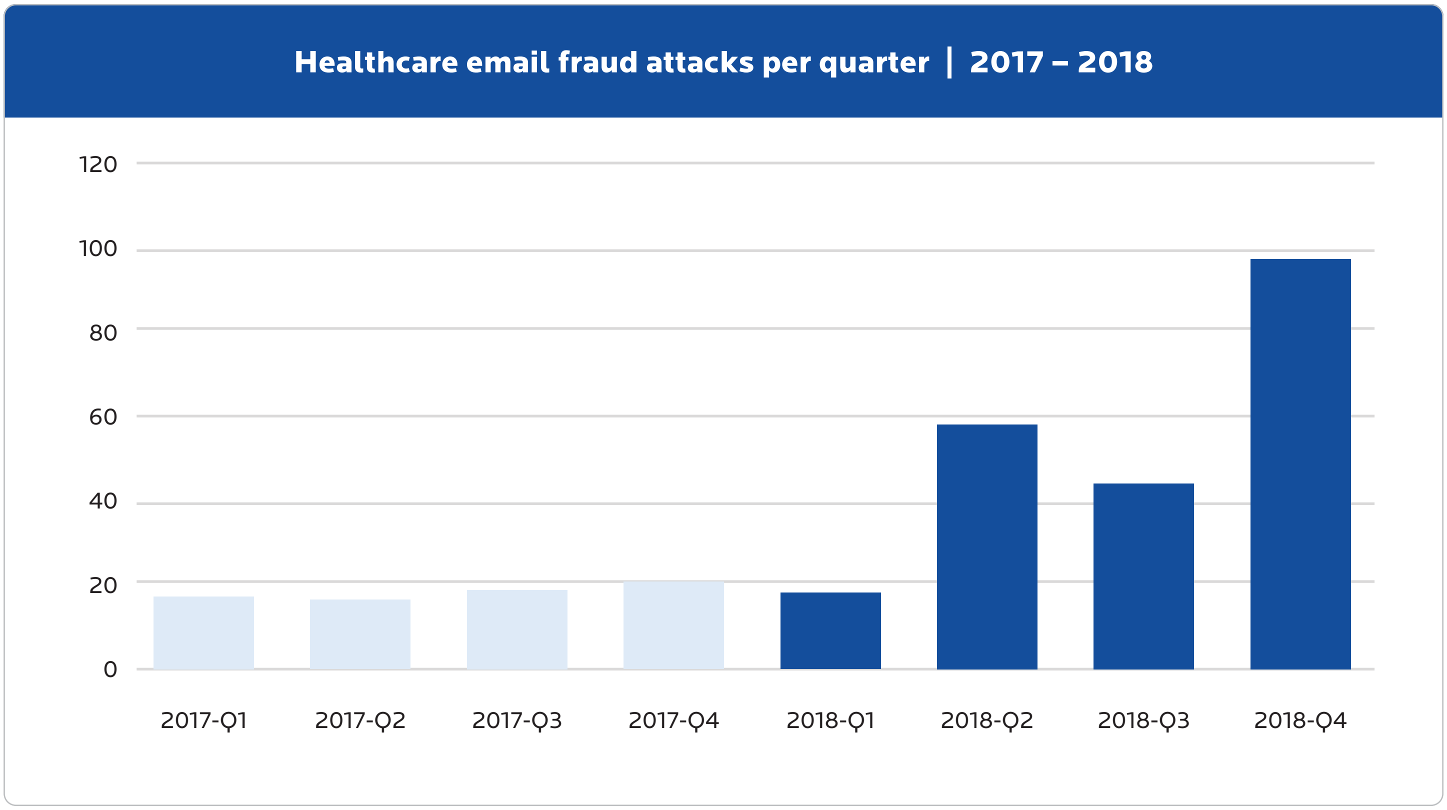


Figure 24: Proofpoint data showing quarterly increases in email fraud attacks against healthcare organizations

Why is healthcare a target?

> The healthcare industry remains one of the top sectors actively targeted by online threat actors, with 89 percent of healthcare organizations reporting a data breach in the past two years. In 2018, Beazley Breach Response found that healthcare suffered the highest number of data breaches across any sector in the US economy, with a reported 41 percent breach rate.

While most health organizations claim to follow cybersecurity practices recommended by a federal task group composed of public and private cybersecurity leaders, organization after organization continue to land themselves into news headlines, either due to a data breach or a ransomware attack. And the one question that comes to mind is: Why?

Why is healthcare so hot in the eyes of hackers right now? After all, several of the largest, highest revenue-generating companies today have nothing to do with the healthcare industry. And yet, not a week goes by, it seems, without another hospital publicly disclosing that they were a target of a cyberattack that crippled their systems. Though cyberattacks against healthcare can be deemed opportunistic because of institutions' weak security postures, cybercriminals wouldn't bother if there wasn't a prize behind those weak walls. Therefore, we have identified three main reasons that make the healthcare sector a prime target of cybercriminals.

Personally identifiable information

Healthcare providers store millions of sensitive patient data points.

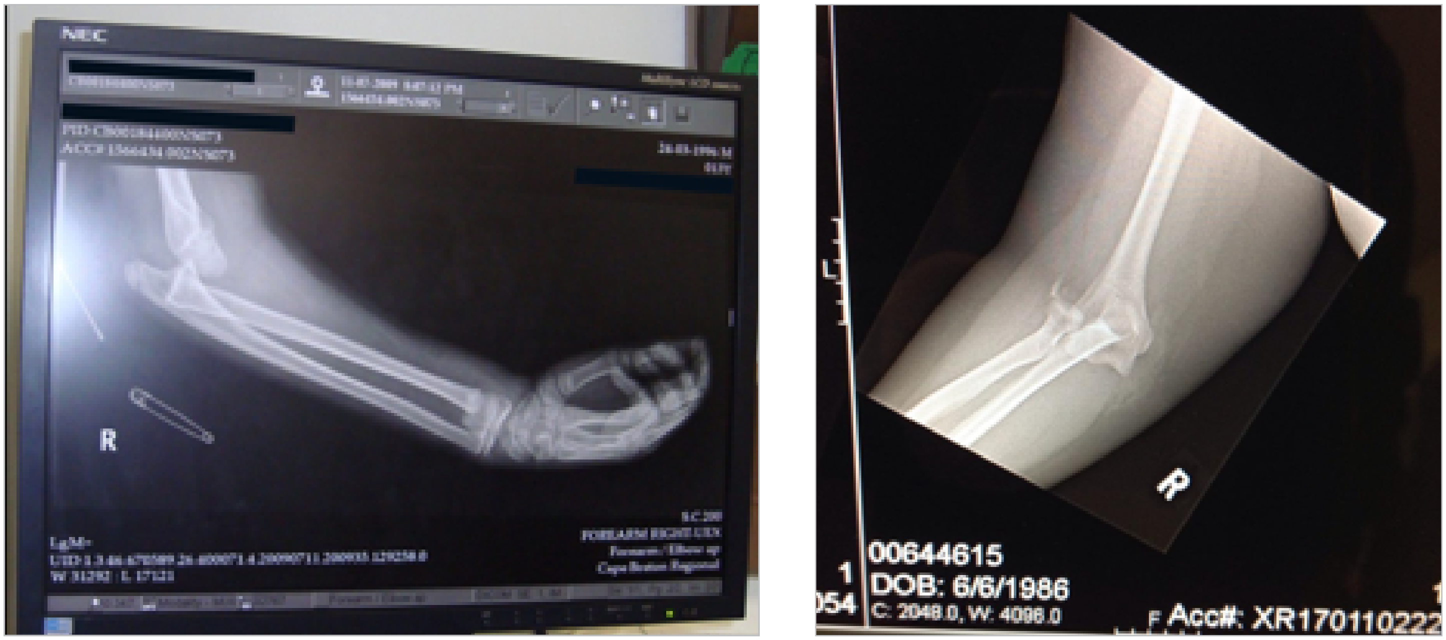
This is the primary reason and certainly the most obvious. To legitimate organizations and cybercriminals alike, data is currency. It's only logical for criminals to target institutions that store thousands, if not millions, of data points on patients and employees.

Patient data of interest to cybercriminals includes the usual personally identifiable information (PII)—complete name, date of birth, family relations, Social Security Number (SSN), addresses, credentials, driver's license numbers, email addresses, phone numbers, and more. In addition, they collect sensitive data related to health that includes health conditions, scans or medical imaging results, blood test results, family and/or genetic history, case history, drug prescriptions, scheduled appointments, food allergies, physicians' diagnoses, notes, and other observations. Such data is rarely found elsewhere.

Cybercriminals can also unearth additional information about a target patient by creating an analytic chain of low-value data. These are pieces of data that, in and of themselves, are non-threatening and wouldn't directly point to a specific person. Cybercriminals can create this analytic chain by using the trivial data they have on hand about a target. For example, an X-ray image contains a patient's name and the hospital's name. Threat actors infer that the hospital name gives away the patient's potential city of residence. This, together with the patient's name, can be used to look up property tax and voting records.

Patient data is highly valuable to underground market sellers.

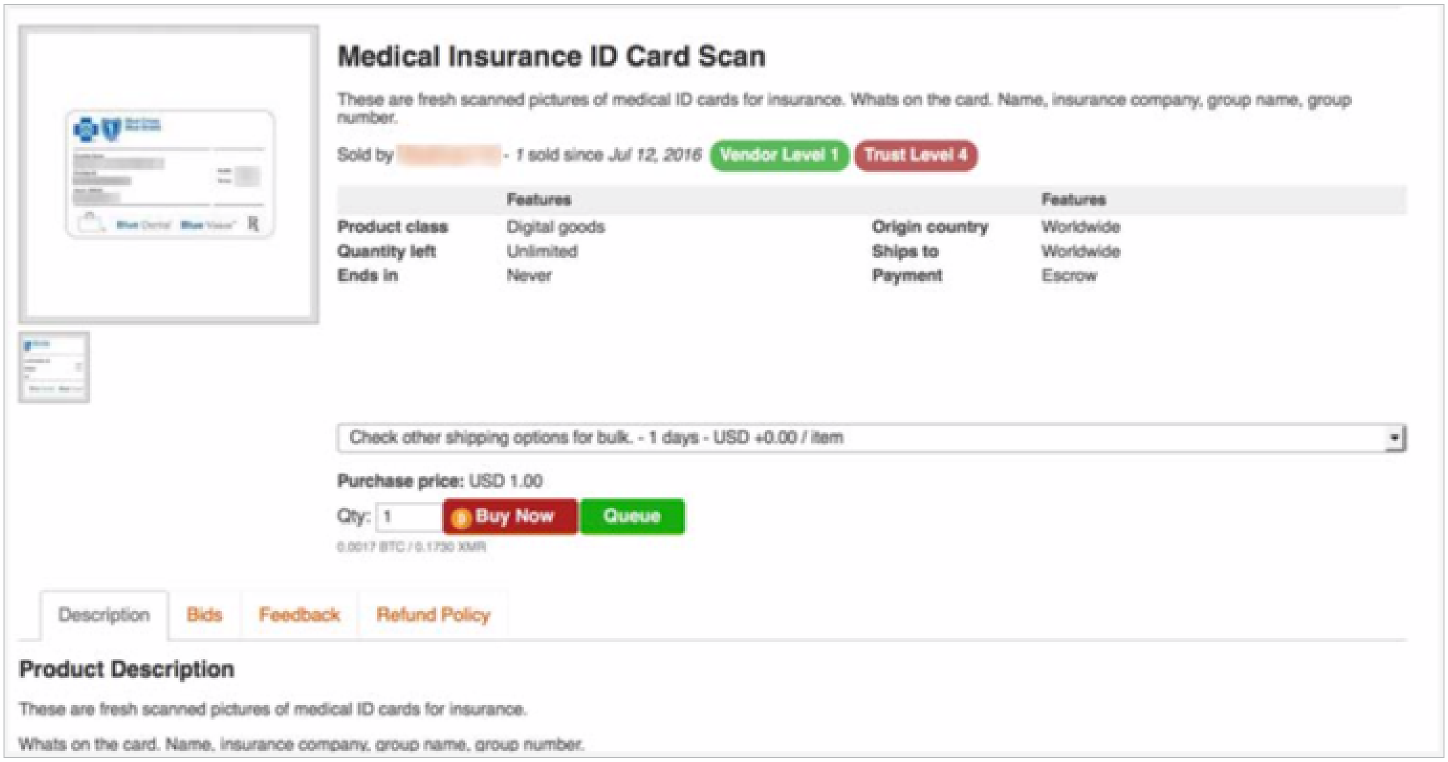
Being able to convert stolen data into money is how threat actors motivate themselves into doing what they do. In cybersecurity, it's common knowledge that stolen PII is sold on the Dark Web, often for a hefty amount of money. In fact, medical information is highly sought after because it can be worth 10 times more than traditional PII. According to a private industry notification from the FBI, a partial electronic



Figures 25 and 26: Patient x-ray scans that show sensitive data, like dates of birth and account numbers

health record (EHR) sells for $50 compared to the $1 price tag on an SSN or a credit card number.

In a 2017 report, it was found that a database of complete EHRs were sold for half a million dollars on the Dark Web. Medical records, being complete data sets, can either be sold whole or in piecemeal, depending on client demands. And fraudsters can use EHR data to further create and sell counterfeit documents like tax returns, IDs, birth certificates, various licenses, and even synthetic identities—which are new, unique identities built from amalgamations of data taken from various individual records. The report goes on to reveal that fake tax returns and birth certificates are prized at $13.50 and $500 each, respectively.



Medical Insurance ID Card Scan

These are fresh scanned pictures of medical ID cards for insurance. Whats on the card. Name, insurance company, group name, group number.

Sold by [redacted] - 1 sold since Jul 12, 2016 Vendor Level 1 Trust Level 4

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Check other shipping options for bulk. - 1 days - USD +0.00 / item

Purchase price: USD 1.00

Qty: 1 Buy Now Queue

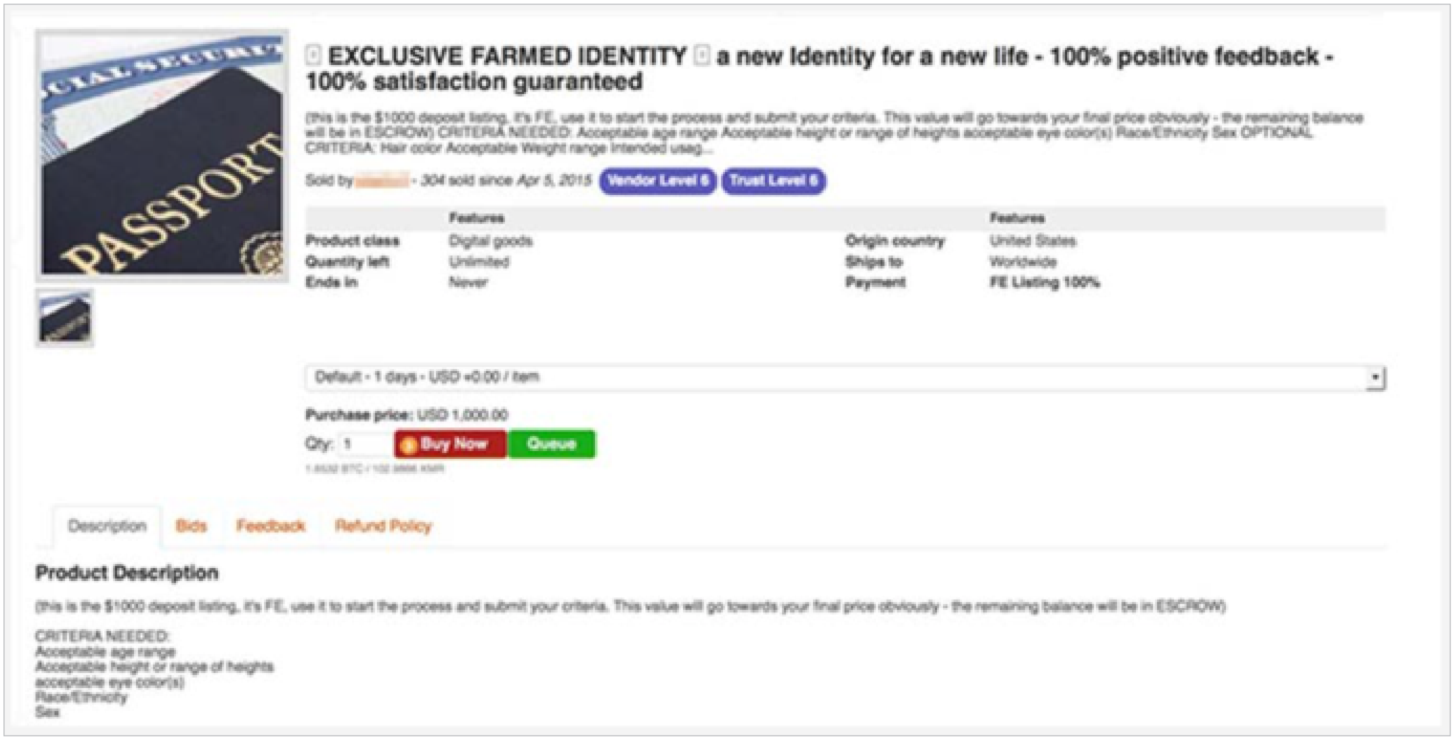
0.0017 BTC / 0.1730 XMR

Product Description

These are fresh scanned pictures of medical ID cards for insurance.

Whats on the card. Name, insurance company, group name, group number.

Figure 27: Ad to purchase medical insurance cards on AlphaBay, a dark web marketplace, in August 2016



□ EXCLUSIVE FARMED IDENTITY □ a new Identity for a new life - 100% positive feedback - 100% satisfaction guaranteed

(this is the $1000 deposit listing, it's FE, use it to start the process and submit your criteria. This value will go towards your final price obviously - the remaining balance will be in ESCROW) CRITERIA NEEDED: Acceptable age range Acceptable height or range of heights acceptable eye color(s) Race/Ethnicity Sex OPTIONAL CRITERIA: Hair color Acceptable Weight range Intended usag...

Sold by [redacted] - 304 sold since Apr 5, 2015 Vendor Level 6 Trust Level 6

	Features		Features
Product class	Digital goods	Origin country	United States
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	FE Listing 100%

Default - 1 days - USD +0.00 / item

Purchase price: USD 1,000.00

Qty: 1

[illegible]

Product Description

(this is the $1000 deposit listing, it's FE, use it to start the process and submit your criteria. This value will go towards your final price obviously - the remaining balance will be in ESCROW)

CRITERIA NEEDED:
Acceptable age range
Acceptable height or range of heights
acceptable eye color(s)
Race/Ethnicity
Sex

Figure 28: AlphaBay advertisement for the sale of a new identity based off stolen data

Assuming identities of real patients allows criminals to buy medical equipment, prescription drugs, or undergo expensive medical services under their victims' names. Not only that, the drugs and equipment they procured can be resold. Some cybercriminals even combine a patient number with a made-up name of a health provider to file medical insurance claims. Such activities can rack up bills that victims will only notice at a later time. And, unlike credit card information, one's birth date, SSN, and medical history are irreplaceable.

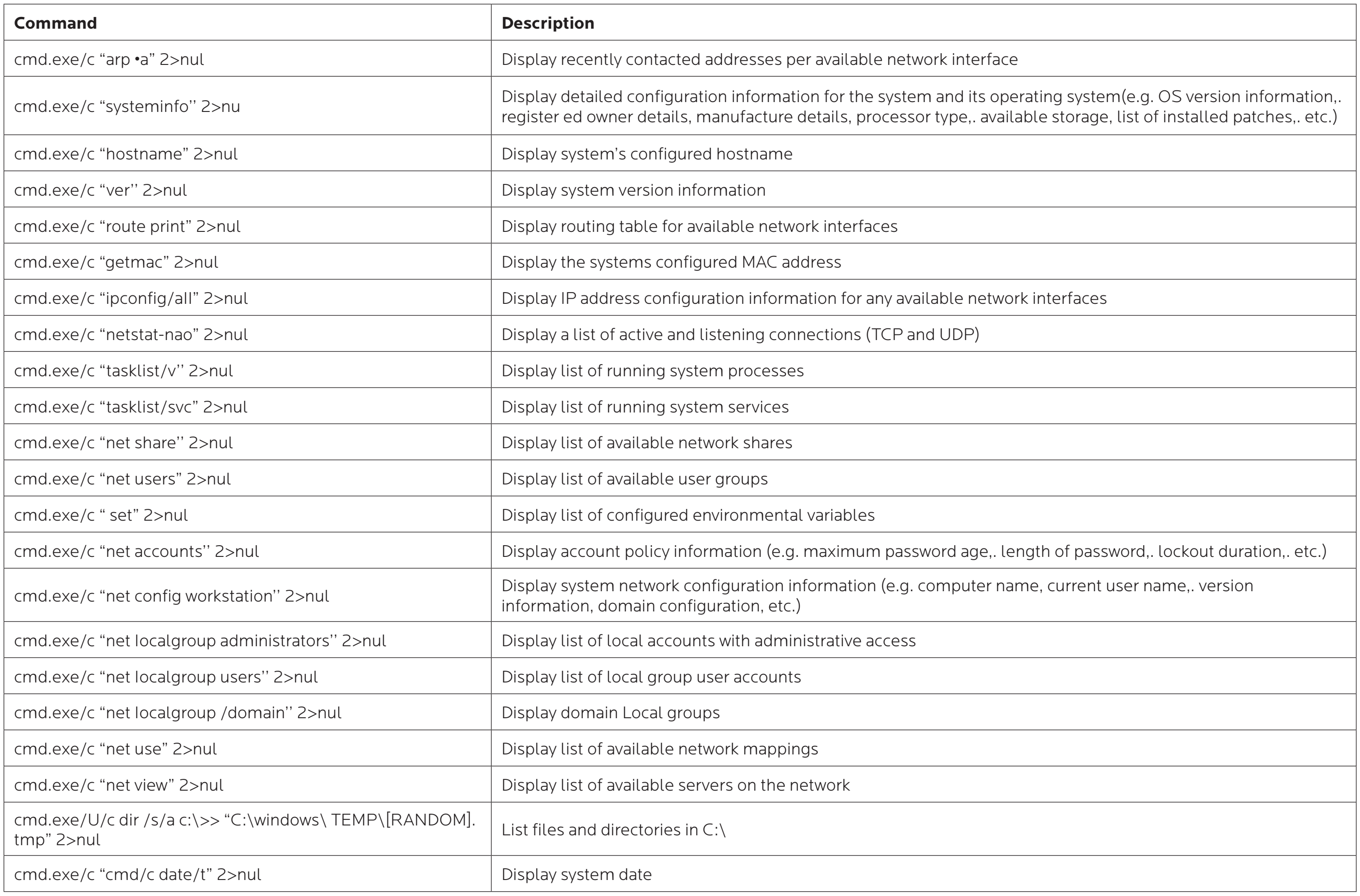
Large number of endpoints

Healthcare organizations have a sizeable number of endpoints.

We're not just talking about desktops, laptops, and tablets that staff use daily to provide care, but also the many medical internet of things (IoT) devices, the personal devices of staff connected to the organization's network, and the varying number of patient and visitor mobile devices that use the hospital or clinic's free Wi-Fi. The number of connected devices of this magnitude means a higher probability of infection and higher infection rate, making them a focal point for potential botnets, reconnaissance activities, or even—hypothetically speaking—a real-world test bed for new malware.

The Internet of Things (IoT) and the implementation of bring your own device (BYOD) policies have fully taken off in institutions across the healthcare industry. Whether it's Internet-connected health-monitoring equipment or a nurse's private cell phone, IoT devices, especially those belonging to staff, are considered inherently insecure. This is because:

1. They are often created by developers who are not trained in producing secure code.
2. They have not baked security into the design of the product itself.
3. They are unable to be protected by security software because they are too specialized.
4. They are a personal device not protected by network or endpoint security.



Command	Description
cmd.exe/c “arp •a” 2>nul	Display recently contacted addresses per available network interface
cmd.exe/c “systeminfo’’ 2>nu	Display detailed configuration information for the system and its operating system(e.g. OS version information,. register ed owner details, manufacture details, processor type,. available storage, list of installed patches,. etc.)
cmd.exe/c “hostname” 2>nul	Display system’s configured hostname
cmd.exe/c “ver’’ 2>nul	Display system version information
cmd.exe/c “route print” 2>nul	Display routing table for available network interfaces
cmd.exe/c “getmac” 2>nul	Display the systems configured MAC address
cmd.exe/c “ipconfig/all” 2>nul	Display IP address configuration information for any available network interfaces
cmd.exe/c “netstat-nao” 2>nul	Display a list of active and listening connections (TCP and UDP)
cmd.exe/c “tasklist/v’’ 2>nul	Display list of running system processes
cmd.exe/c “tasklist/svc” 2>nul	Display list of running system services
cmd.exe/c “net share’’ 2>nul	Display list of available network shares
cmd.exe/c “net users” 2>nul	Display list of available user groups
cmd.exe/c “ set” 2>nul	Display list of configured environmental variables
cmd.exe/c “net accounts’’ 2>nul	Display account policy information (e.g. maximum password age,. length of password,. lockout duration,. etc.)
cmd.exe/c “net config workstation’’ 2>nul	Display system network configuration information (e.g. computer name, current user name,. version information, domain configuration, etc.)
cmd.exe/c “net localgroup administrators’’ 2>nul	Display list of local accounts with administrative access
cmd.exe/c “net localgroup users’’ 2>nul	Display list of local group user accounts
cmd.exe/c “net localgroup /domain’’ 2>nul	Display domain Local groups
cmd.exe/c “net use” 2>nul	Display list of available network mappings
cmd.exe/c “net view” 2>nul	Display list of available servers on the network
cmd.exe/U/c dir /s/a c:\>> “C:\windows\ TEMP\[RANDOM]. tmp” 2>nul	List files and directories in C:\
cmd.exe/c “cmd/c date/t” 2>nul	Display system date

Figure 29: A screenshot of commands executed by Orangeworm within victim environments

IoT devices represent a substantial risk to a network where EHR and personal health records (PHR) reside. And the threat is real. According to a recent survey by security software company Irdeto, 82 percent of healthcare organizations have faced an IoT-focused cyberattack in the past year.

Medical IoT devices offer new ways to monitor patients and equipment while improving care and lowering costs. But many of these smart devices have unknown security protections. Connected medical devices—from Wi-Fi enabled infusion pumps to smart MRI machines—increase the attack surface of devices sharing information and create security concerns including privacy risks and potential violation of privacy regulations.

For example, in 2018, Symantec researchers discovered a group of threat actors called “Orangeworm” that had been deploying the Kwampirs backdoor into healthcare industry machines. The malware was found on X-ray and MRI machines.

Third-party devices like phones, tablets, and portable gaming consoles belonging to staff, patients, and visitors, directly contribute to the ballooning number of computing devices connecting to an institution’s network. Unfortunately, they are unregulated and are deemed non-compliant in terms of how secure they are themselves. It’s not only staff that use a healthcare institution’s network, either. Also given access are physicians employed by outside, independent medical groups that work onsite at multiple facilities and medical students that have access to sensitive patient data for academic purposes.

Cybercriminals will no doubt opt to target 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.

Best ROI in the business

Attacking healthcare institutions is a surefire return on investment for cybercriminals.

Cybercriminals know that healthcare institutions heavily rely on PHI in normal day-to-day operations. Capturing and holding for ransomware these records—along with backups and program files local to systems and devices that make them work—is guaranteed to halt normal operations and, consequently, put patients in critical care on a timer. Payout is expected to be swift and guaranteed, especially when healthcare organizations, which are normally ill-prepared and ill-equipped for such attacks, scramble to get their data and files back quickly. Otherwise, any added downtime could result in permanent health damage to patients.

A recent Coveware analysis showed that not only did the average ransomware demand rise 184 percent to $36,295 from the Q2 2019, but that the healthcare industry accounted for 13.6 percent of ransomware targets.

These all make the problem of cybersecurity more challenging and complex to address. Institutions may comply to standard guidelines. Policies may be set and are expected to be followed by everyone. But the likelihood of persons or groups inadvertently violating them is high when the focus is on providing optimal care to patients.

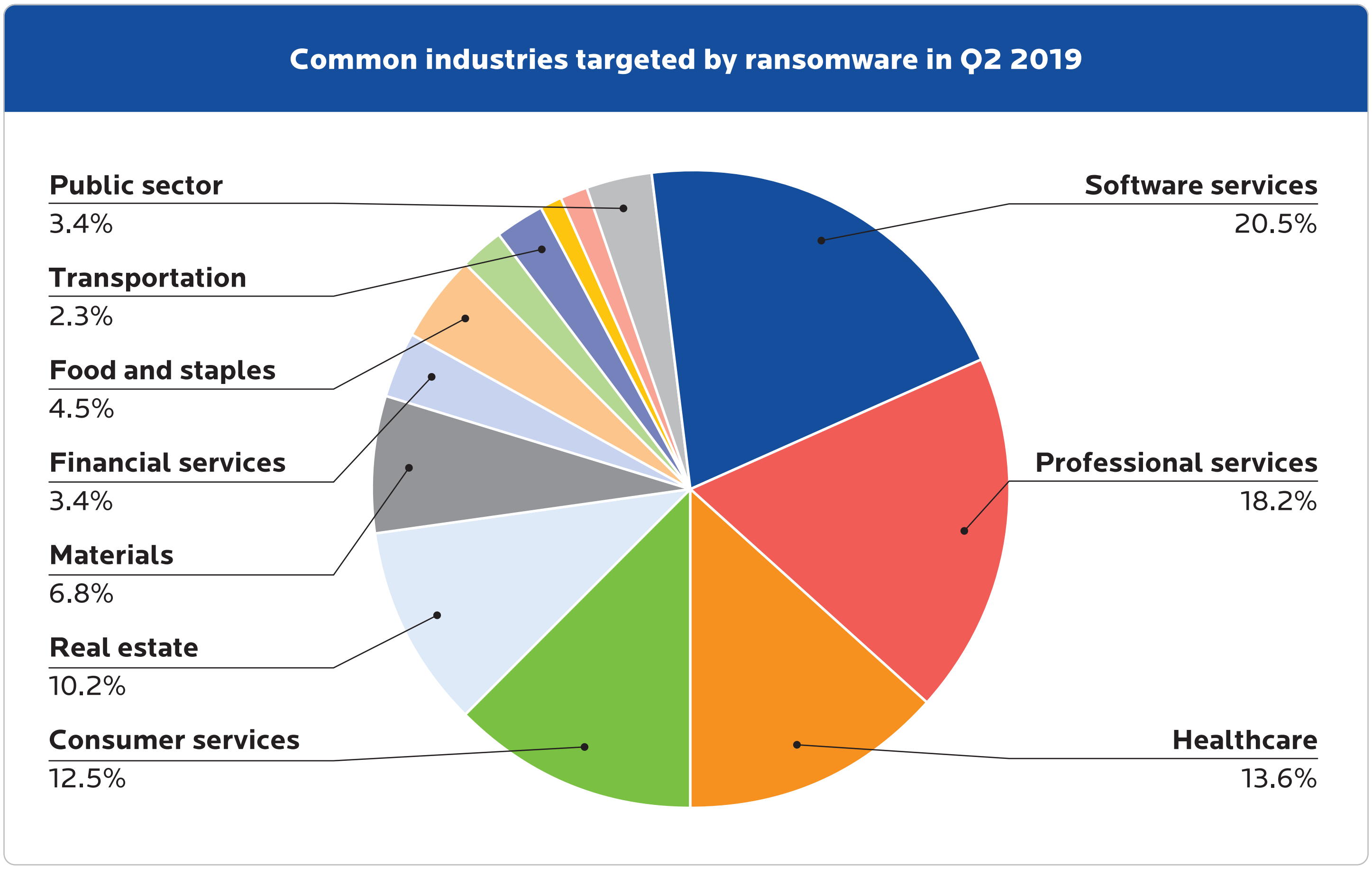


Figure 30: The healthcare industry accounted for 13.6 percent of ransomware attacks in Q2 2019

Security challenges in healthcare

> The many cybersecurity and privacy challenges the healthcare industry is facing aren’t enough to hamper it from adopting emerging technologies. Actually, this spurs healthcare industry members into grappling with what these technologies can do for them now and how they could potentially address future problems. Artificial intelligence (AI), blockchain, and virtual reality are just some of the current technologies the sector is willing to embrace, not only to take care quality to the next level but also tighten privacy and cybersecurity defenses in organization networks and systems.

Indeed, improvements are on the way; however, the current state of security in healthcare has a long way to go. Next, we look at some of the current and longstanding security issues that continue to challenge the healthcare industry beyond negligence, hacking, and malware.

Legacy systems

The sustained use of legacy and unsupported systems is considered one of the top reasons why healthcare remains an easy target for cyberattacks.

According to a survey by Merlin International and the Ponemon Institute in 2018, of more than 600 healthcare executives surveyed, 58 percent believed that the reliance on legacy systems increased the vulnerability of their patients’ information.

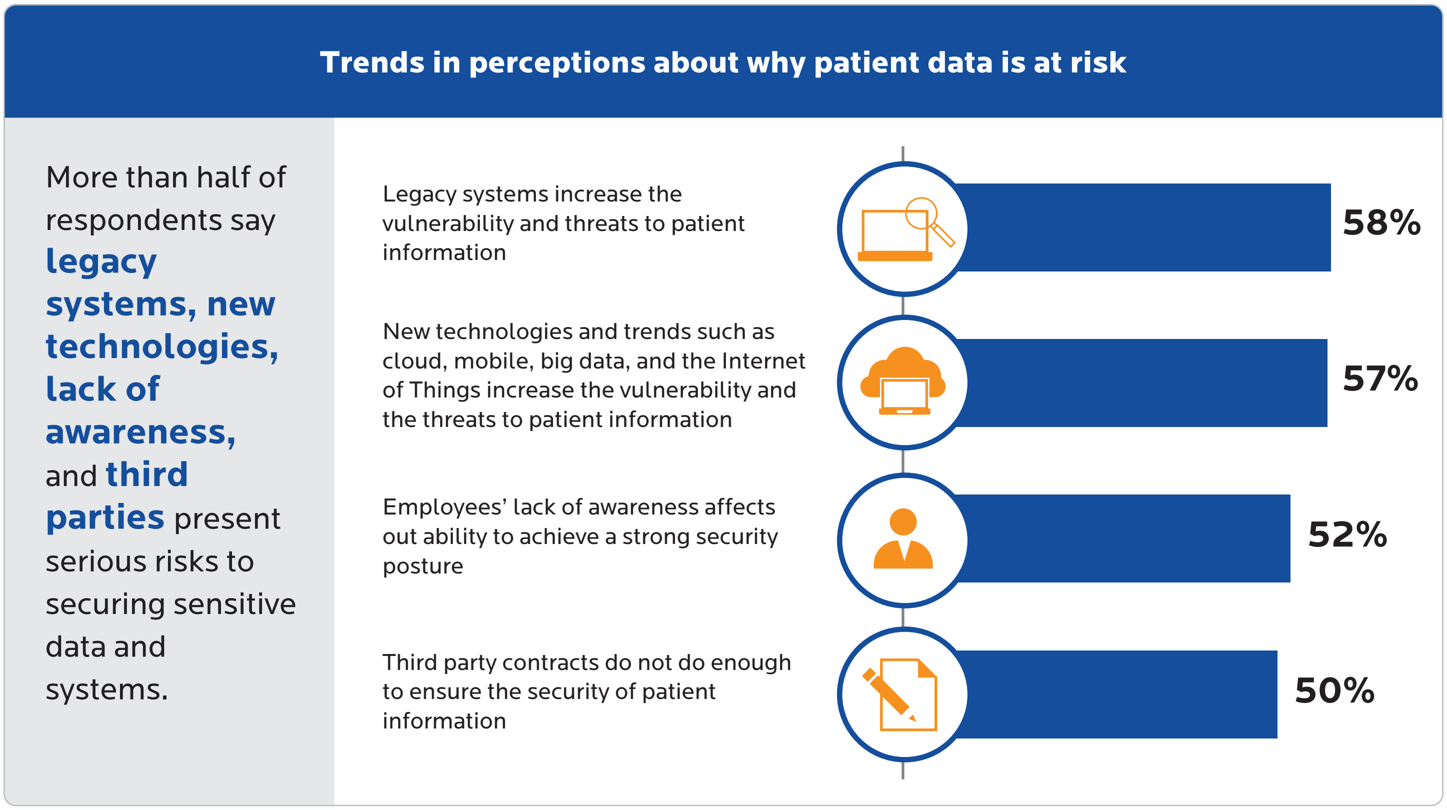


Figure 31: Healthcare executives share their thoughts on the risks to their patients’ information

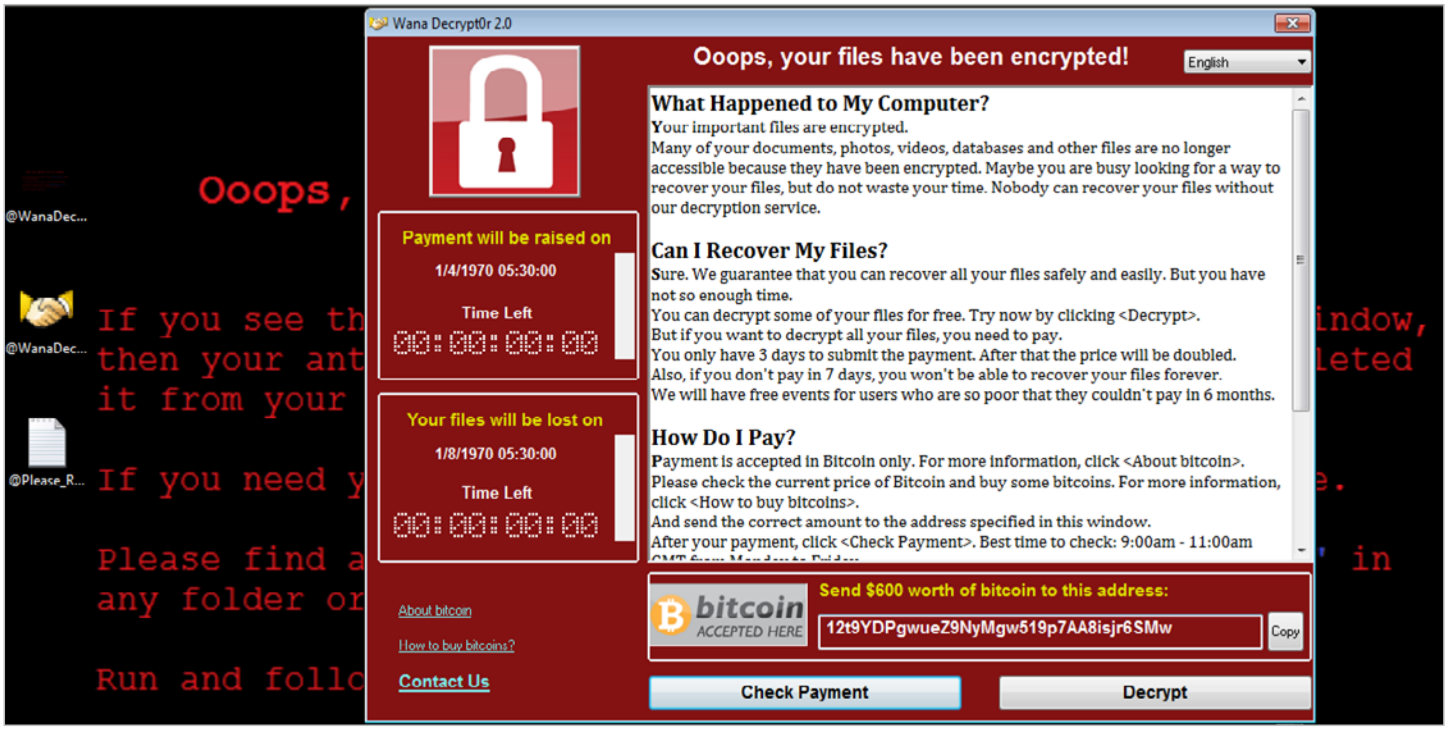
In Canada, Sarah Jamie Lewis, executive director of Open Privacy Research Society, discovered that the Vancouver Coastal Health Privacy Office (VCH-P) was unknowingly broadcasting unencrypted sensitive medical information of patients via its old paging system. According to the society's press release, information being broadcast included "the patient's name, age, gender marker, diagnosis, their attending doctor and room number. Other broadcasts regarding medical tests such as x-rays are often associated with a patient's last name or medical number, exposing their progression through hospital departments." VCH-P, like many healthcare organizations, continues to play catch-up with tech and admits that they will replace it but this will take time. Upgrading is a slow-going, difficult, and expensive undertaking, but if left unattended, patients, staff, and the business itself will continue to take the full brunt of cyberattacks.

Arguably, some machines and devices aren't PCs and cannot be upgraded, either due to hardware limitations or the cessation of firmware support. But for PCs continuing to run on legacy systems, which will soon include Windows 7, upgrading is no longer an option but a requirement. Just think about the different impact of WannaCry on the UK's National Healthcare Service (NHS) if a third of their affected systems had already been running on Windows 10. Think about WannaCry's impact on disrupted NHS Trusts if they had actually applied the patch that could have stopped the ransomware from proliferating and wreaking havoc. More importantly, how successful could this ransomware have been if NHS staff were trained on basic cybersecurity best practices?

Cybersecurity posture needs defibrillation

Under-resourced IT and security

While it is true that more healthcare organizations are increasing their budget for IT and security spending, this is for the procurement of more advanced medical devices and systems. This doesn't include staff training or the hiring of more IT personnel to oversee their technological assets, making sure that the server, endpoints, and network are functioning normally and not showing signs of disruption from external sources.



Ooops, your files have been encrypted!

Payment will be raised on
1/4/1970 05:30:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 05:30:00
Time Left
00:00:00:00

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 32: A screenshot of the WannaCry ransomware attack once it has infected a machine

When staff aren't trained properly or are under-resourced, the end result is negligence. This is almost always unintended, but is the result of a systematic failure by the healthcare industry to prioritize cybersecurity at every level. We continue to see WannaCry infections in our product telemetry on healthcare institutions because the SMB vulnerability famously exploited in the 2017 ransomware outbreak has still not been patched by organizations globally, even though National Health Service (NHS) in the UK fell public victim to it on day 1.

WannaCry ransomware made a name for itself after affecting thousands of systems across a wide range of sectors worldwide. For the healthcare industry, it was a watershed moment. Although WannaCry wasn't intended to target the NHS, it created severe disruptions and life-threatening risks the UK had to desperately grapple with for days. And yet, it remains unpatched on systems today.

In 2018, ratings firm SecurityScorecard ranked healthcare 15th out of 17 industries in security posture, citing poor patching cadence as the reason for 60 percent of the cybersecurity issues plaguing the medical field. A weak security posture and poor patching cadence are likely the result of overtaxed or undertrained healthcare IT staff, coupled with lack of security resources to get the job done, and done well. While hospital budgets are mostly reserved for research, patient care, or technological innovations, it bears repeating that the primary budget decision makers in the medical field—especially its board of directors and chiefs of staff—must divert some funding for security staff, equipment, training, and defense software and services, otherwise continue to be picked off by opportunistic threat actors.

Little-to-no cybersecurity awareness and training

It's no surprise to see that healthcare institutions that continue to ignore their cybersecurity problem are also keeping all their staff in the dark when it comes to dangers and potential risks that threaten them daily. Because of this, staff members have no idea when they're face-to-face with a phishing email. Such naivete and the lack of awareness of online threats and basic computing hygiene are the end-results of under-investment in personnel training.

Cybersecurity, in general, typically takes a backseat because it doesn't generate revenue for the organization. Healthcare institutions would rather focus their investments on research and technologies that enhance the quality of the patient's overall care journey. This is beginning to change, looking at the last 12 months. According to a recent survey from the Healthcare Information and Management Systems Society (HIMSS), the healthcare sector has been making many positive strides towards improving their security posture by allocating more of their IT budget to cybersecurity. Unfortunately, only a few companies focus on improving staff training.

Budget is not the only resource lacking in an institution's IT and security department. There are also people. Like any other sector, healthcare is similarly experiencing a cyber skills gap. The same Merlin International and Ponemon Institute study referenced above showed that more than half of their respondents said it was either "difficult" or "extremely difficult" to recruit IT professionals in their field. A full 73 percent said the "insufficient staffing" challenged their organization's cybersecurity posture from being "fully effective."

If organizations are struggling to find qualified cybersecurity professionals to fill in new positions, replacing them is equally challenging. The demand for Chief Information Security Officers (CISOs), information security analysts, and computer support specialists (among others) are forecasted to increase, along with their pay grades and the ever increasing challenge of security systems, networks, and people. Indeed, the mounting pressure to shore up defenses of healthcare organizations has never been higher. Unfortunately, the longer positions are left open, the greater the stress on an institution's IT and cybersecurity team. With potentially more work and longer work hours, plus an already lean staff, this could lead to rising stress levels, burnout, and mental health concerns.

Lack of network segmentation

It's crucial for institutions who house thousands of extremely sensitive data points to at least create some sort of barrier between these data and unauthorized parties. One of the best ways of doing this is network segmentation, or the practice of splitting the network into subnetworks. Doing so will improve performance. Further, threats that may be introduced by anyone connecting to the healthcare facility's internet may not necessarily be the same threats against a network that can only be accessed by authorized individuals.

Leaky data

In the case of Canada's VCH-P that we saw earlier, it's conceivable for legacy systems to cause inadvertent leaking of sensitive patient data. But the problem of leaky data is also present in modern technology.

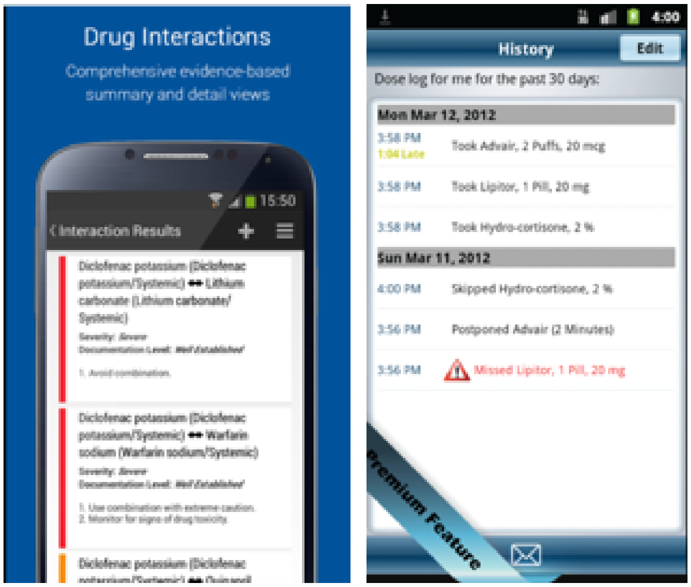
In response to the wave of digitizing data for easy sharing of patient medical records, many institutions—including those in healthcare—avail themselves of services that offer data storage, may it be in the cloud or on-premise, to address their accessibility and storage needs. These storage servers are called PACS, and they are usually public-facing but should only be accessible by trusted parties with credentials. Sadly, misconfigurations in cloud settings and framework implementation errors can set the stage for a "self-breach", or the accidental breaching of sensitive and confidential data by an individual or an organization's own hand.

Take, for example, the case where default credentials of the PACS server remained usable in accessing a purportedly restricted portal full of sensitive patient information. Modules for authentication in accessing PACS servers remain deactivated—a fault we can put squarely on the shoulders of the team who set up the servers and on the developers behind the software used in these servers—even after the institution began using them.

Insecure third-party medical management apps

Mobile apps are not exactly the most secure of software, yet they offer convenience, immense ease, accessibility, and flexibility that oftentimes one can't do without in a fast-paced and busy world. Third-party vulnerabilities do not only extend to healthcare institution-facing software, but also to 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—thus increasing the overall attack surface for cybercriminals. In addition, the presence of advertising or analytics trackers increases processing time, which could increase the app's vulnerability to breach.

Finally, medical apps are not required to be HIPAA compliant, further increasing the odds for attack. Researchers this year found that multiple mobile medical management apps shared user data of various kinds with third parties, enlarging the attack surface even more. In fact, because of the sheer amount of data moving through the app, there's a chance that cybercriminals needn't even breach the program, but instead can let the data come to them. In an article for Malwarebytes, healthcare penetration test Mike Jones said that a huge concern with medical management apps is data leakage.



Drug Interactions

Comprehensive evidence-based summary and detail views

15:50

Interaction Results

Diclofenac potassium (Diclofenac potassium/Systemic) ↔ Lithium carbonate (Lithium carbonate/Systemic)
Severity: Severe
Documentation Level: Well Established
1. Avoid combination.

Diclofenac potassium (Diclofenac potassium/Systemic) ↔ Warfarin sodium (Warfarin sodium/Systemic)
Severity: Severe
Documentation Level: Well Established
1. Use combination with extreme caution.
2. Monitor for signs of drug toxicity.

Diclofenac potassium (Diclofenac potassium/Systemic) ↔ Quinapril

4:00

History

Edit

Dose log for me for the past 30 days:

Mon Mar 12, 2012

3:58 PM 1:04 Late — Took Advair, 2 Puffs, 20 mcg

3:58 PM — Took Lipitor, 1 Pill, 20 mg

3:58 PM — Took Hydro-cortisone, 2 %

Sun Mar 11, 2012

4:00 PM — Skipped Hydro-cortisone, 2 %

3:56 PM — Postponed Advair (2 Minutes)

3:56 PM — ⚠ Missed Lipitor, 1 Pill, 20 mg

Figures 33 and 34: Screenshots of the medical management apps MIMS and Dosecast, both of which were found to share user data

Once attackers gain access to these apps, they can do whatever they want with the data, such as selling to the highest bidder, tampering with them, or using them for fraudulent purposes.

According to CHiMe Healthcare's Most Wired 2018 National Trends report, only 29 percent of healthcare organizations reported having a comprehensive cybersecurity program. In addition, 10 percent of organizations lacked mobile device management. As more and more devices are plugged into healthcare facility networks, operating without a security management plan significantly increases the susceptibility of networks to breach, jeopardizing normal hospital operations and endangering patient safety.

Unsecured APIs

An application programming interface (API) is a piece of software that allows two different programs to talk to each other. Unfortunately, not all APIs area developed with the same care and security consciousness as they should be. As a result, hackers can exploit their weaknesses to gain access to a healthcare organization's network and cause a data breach.

The American Hospital Association (AHA) released a 2019 report recognizing the severity of this risk, thus advising mobile healthcare stakeholders to create a secure app environment for the parties to exchange health data. In April 2019, the Office of the National Coordinator for Health Information Technology (ONC) released a second draft of the Trusted Exchange Framework and Common Agreement (TEFCA) outlining key considerations for the privacy and security of healthcare APIs. However, the TEFCA is entirely voluntary—especially for third-party apps that needn't be HIPAA compliant.

Needs stitches

A restrictive update process for many medical software programs may make it difficult to stay on top of security patches.

Electronic medical record software companies helped usher in the age of digitization for the healthcare sector, with some becoming billion-dollar companies. Unfortunately, with their rise comes unintended consequences that may be good in the business's perspective but are limiting for the very clients they're serving. Healthcare software, for example, can only be serviced by the vendor itself. This in turn creates delays in software maintenance, such as patching—a process that could have benefited from automation—leaving affected systems open to vulnerability exploitation until after service from the vendor.

Hard-coded credentials on physical medical devices

If many see problems in old medical devices, expect to see them in modern ones, too. Case in point: Several medical devices from different manufacturers were found to contain hard-coded credentials in them, usually passwords. As the presence of hard-coded credentials takes the difficulty in guessing away from the attackers, patient data is at risk if attackers or malicious actors gain access to the operating systems and their product development code and, eventually, take full control over the device.

Little-to-no coordinated medical device security management plan

As more and more devices are getting plugged into a network, healthcare facilities still operate without a medical security management plan in place, significantly increasing the susceptibility of its network being exploited, jeopardizing normal hospital operations, and endangering patient safety.

Consequences of a breach

> Like any other sector, healthcare must realize that when they use computing devices, keep troves of sensitive information, and leverage the internet—in any way—to deliver optimal patient care, they are at risk of cyberattacks. Accepting this is key. Only then will healthcare truly begin to recognize and understand the threats they face and come up with effective ways to protect themselves, now and into the future. The cumulative value of what's at stake is too high to put a price tag on and too disparaging to life to leave to chance.

We know that cyberattacks on healthcare institutions usually result in loss of sensitive data. However, not all attacks are aimed at stealing or ransoming data.

Researchers at Ben-Gurion University had postulated that highly sophisticated attackers could be targeting data to manipulate. These researchers then developed malware that can affect scans taken from CAT and MRI scanners. It can add fake tumors on an otherwise clean scan, and it can remove signs of tumors on scans that otherwise show a patient's life-threatening illness. The end result? Both doctor and patient are fooled into thinking that sick patients are well and healthy patients need treatment. These devastating misdiagnoses could cause fear and anxiety or, worse, end a life.

If data can be lost in the event of an attack, productivity is lost, too. On top of this, the service is severely disrupted. Hospital staff are compelled to revert to using pen and paper when filing, recording, and monitoring patient progress. Often, affected hospitals are forced to turn away all new, non-critical patients and redirect them to other hospitals. This is disastrous, and highly indicative of a lack of planning and disaster recovery protocols.

Surgeries and other procedures could also be postponed or cancelled in the event of an attack. Moving critical patients in immediate need of surgery to the nearest available hospital would be another obstacle.

Let us also not forget that not all organizations in healthcare deal with medical information. There are also companies that deal with care institutions themselves. The Blue Cross of Idaho, for example, is a health insurer that was hit by a data breach in April 2019. They detected in March 2019 that an unauthorized party attempted to reroute a financial payment intended for a healthcare provider. In the case of Palmetto Health, which also detected a breach in March 2019, they believed that an unauthorized party aimed to gain access to payroll information.

A ransomware hit is something every healthcare institution dreads—and for good reason. Apart from the operational problems associated with having all crucial files encrypted, systems shutting down, and the time and effort it takes to bring back normalcy, healthcare institutions can also be faced with a severe budget hit should they decide to pay the ransom demand—as insurance does not always cover ransomware attacks—and get things back a lot more quickly.

But what's probably more frustrating to law enforcement, who advises organizations to never pay the ransom no matter what, some may be forced to pay up due to legal requirements and solid adherence to service-level agreements (SLAs). It is always possible that the legal cost for breaking an SLA would be higher than the ransom demand. If one would then opt for the lesser evil, addressing the ransom would be preferred.

Lastly, a ransomware attack can also force owners of certain healthcare facilities, especially small- to-medium-sized firms, to permanently close their doors. When Wood Ranch Medical in California was hit by a ransomware attack in August, the provider had to shutter its doors, unable to rebuild and recover health records from backups. Last year, the Brookside ENT and Hearing Center in Michigan shut its doors after ransomware threat actors wiped their entire system, deleting all electronic patient records, because they refused to pay. Patients of these affected care providers would have to rebuild their medical records with another practice. Unfortunately, certain details that only the affected care provider would have records of, such as details about a surgery, can never be provided to the new practice as those have been lost.

Future concerns

> Technological innovation in healthcare is happening at a breakneck pace. In just two years, discoveries in the field of genetics have led to life-extending treatments for cancer patients who previously faced grim prognoses. Advancements in prosthetics range from robotic limbs allowing for more refined movement to surgical techniques using muscle grafting and existing nerves, which could help patients actually feel their artificial appendages. Yet the future developments in healthcare that keep security researchers up at night are much less controversial as many other biological breakthroughs, such as stem cell research or cryogenics. Instead, some of them are as mundane as providing convenience for doctor and patient care, whether by allowing for remote/video visits or using IoT to assist in procedures. Below are a few areas of innovation where we already see cybersecurity faltering, and fear future ubiquitous adoption could erode what little security measures healthcare organizations have in place.

Large databases of DNA: a security and privacy concern

Large databases of DNA, collected by the likes of 23andme or Ancestry.com, are already being used for scientific and pharmaceutical research, as all who submit to a genetic test must either consent to allowing such research or having their samples destroyed. While many of the consumer DNA testing kit companies follow privacy and security best practices for storing their data, that doesn't change the fact that, if breached, thousands if not millions of users' DNA could end up in the hands of cybercriminals. And while DNA isn't currently fetching top dollar on the black market, one need only use their imagination to consider a future in which stolen DNA leads to nearly impossible-to-correct identity theft, or worse, the DNA of a wrongly-accused victim planted at the scene of a crime.

In addition, law enforcement routinely ask for and are granted access to these databases, and they can be used to find criminals who aren't even part of the system (but whose relatives are), as was the case for the Golden State Killer. Human rights advocates routinely protest the collection of DNA in databases for fear of future biosurveillance. This is already happening in countries such as China, and in the United States, the White House has announced plans to collect DNA of migrants in federal immigration custody.

Proliferation of IoT: collecting even more data, still not secured

The Internet of Things has already revolutionized healthcare, allowing for patients to dial in to appointments with their doctors from their mobile phones—and the comfort of their couch. Patients can take pictures of their rashes and send data to doctors from wearable devices, including heart rate, blood pressure, or glucose levels, allowing doctors to monitor their vitals or progress on a health goal without having to endure long hospital stays or repeated visits to the office. Physicians and hospitals, meanwhile, use IoT to keep track of patients and medical equipment, facilitate pharmaceutical orders, or prevent infection from spreading via IoT-enabled hygiene devices.

IoT and the widespread embrace of electronic health records (EHR) has already disrupted the healthcare industry, allowing for real-time interconnectivity of patient data, devices, and medical applications through the cloud—yet none of these devices have been properly developed with security by design. Furthermore, as new IoT devices are developed and more and more people use them for healthcare applications, the data collected, transmitted, and stored in the cloud will number in the trillions. Already, new Big Data technologies are looking at aggregating and parsing healthcare data for the purpose of study. That's a giant flame that'll surely attract many, many moths.

Figure 35: Precision IoT instruments use AI to guide robotic surgical arms.

Whether through weak code, vulnerable software, or because the devices are too niche or new to have associated security solutions, cybercriminals will become even more adept at compromising anything IoT. Consider the consequences of trillions of health data points in the hands of threat actors. Could they be modified to skew test results? Could the devices be mobilized into a botnet army? Which key operations could come to a screeching halt? IoT developers and healthcare organizations, then, must consider security as they innovate and implement, otherwise face certain compromise.

Internet of Thoughts: weaponization of AI and ML

While it may seem like the subject of science fiction, brain-machine interface (BMI) technology is a field in which dedicated, big-name players are looking to develop a wide variety of applications for establishing a direct communication pathway between the brain and an external device. Some of these players are primarily interested in healthcare-centric implementations, such as enabling paralyzed humans to use a computer, but for others, improving the lives of the disabled are simply short-term goals on the road to much more broad and far-reaching accomplishments.

One such application of BMI, for example, is the development of a Human Brain/Cloud Interface (B/CI), which would enable people to directly access information from the Internet, store their learnings on the cloud, and work together with other connected brains, whether human or artificial. B/CI, often referred to as the Internet of Thoughts, imagines a world where instant access to information is possible without the use of external machinery, such as desktop computers or mobile phones. Search and retrieval of information will be initiated by thought patterns alone.

At some level, brain-machine interface technology already exists today. For example, there are hearing aids that take over the function of the ears for people who are deaf or hard of hearing. These hearing aids connect to the nerves that transmit information to the brain, helping people translate sound they'd otherwise be unable to process. There are also several methods that allow mute or paralyzed people to communicate with others, although those methods are still crude and slow. However, organizations are moving quickly to transform BMI technology from theoretical to practical.

One company working on technology to link the brain to a computer is Elon Musk's startup Neuralink, which expects to be testing a system that feeds thousands of electrical probes into the human brain in 2020. Neuralink's initial goal is to help people deal with brain and spinal cord injuries or congenital defects. Such a link would enable patients to use an exoskeleton, but the long-term goal is to accomplish a brain-to-machine interface that could achieve a symbiosis of human and artificial intelligence.

The applications for BMI technology are nearly endless. However, there are countless concerns about the ethical development of this technology—and even more from a security standpoint. For example, how will BMI integrate with hospital systems that use legacy software? Is it even possible to secure an Internet-connected human brain? What are the implications of a cybercriminal actually hacking BMI or B/CI? Cybercriminals are already learning how to use AI and machine learning (ML) against security solutions—what if they could weaponize AI to take control of a person's exoskeleton to conduct violence; or worse, use malicious AI to modify people's thought patterns? Privacy will also be a huge issue, since a cloud-connected brain could accidentally transmit information we'd rather keep to ourselves. Without pausing to consider ethical and secure development of these future technologies, all of the above wild sci-fi nightmare scenarios could come true.

Conclusion

> Cyberattacks against healthcare organizations are increasing as we head into 2020, especially those leveraging dangerous threats such as TrickBot and ransomware. Meanwhile, healthcare as an industry suffers from a weak cybersecurity profile, despite being covered by regulations such as HIPAA. Budgets are diverted to research, patient care, and technology innovation, while ignoring necessary staff training and solutions for endpoint and network security. Add to this the proliferation of electronic health records and IoT, and you have a prescription for cyber chaos. This is especially concerning when you consider the consequences of a breach on healthcare institutions: disruption of care could ultimately cost patient lives.

But just because healthcare cybersecurity is circling the drain doesn't mean we have to call it just yet. Future federal or state legislation regulating IoT or third-party medical management apps could better protect patient data, especially if a GDPR-like statute is passed in the United States. In addition, if IT directors can make the case to hospital boards for increased security budgets, then a larger number of trained staff could strengthen cybersecurity postures and implement employee awareness programs, deflecting many of the attacks that are successful today. If the security industry can also press IoT and app developers to embrace secure code and API practices, there's cause to be optimistic for an excellent prognosis for medical cybersecurity in the future.

Contributors

Adam Kujawa
Director of Malwarebytes Labs

Wendy Zamora
Editor-in-chief, Malwarebytes Labs

Jovi Umawing
Senior Threat Content Writer

Pieter Arntz
Senior Threat Intelligence Analyst

David Ruiz
Threat Content Writer

malwarebytes.com/business   corporate-sales@malwarebytes.com   1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.