Carbon Black.

Healthcare Cyber Heists in 2019

20 leading CISOs from the healthcare industry offer their perspective on evolving cyberattacks, ransomware & the biggest concerns to their organizations

Rick McElroy, Head of Security Strategy, Carbon Black
Tom Kellermann, Chief Cybersecurity Officer, Carbon Black

JUNE 2019

Executive Summary

The phrase, "First, do no harm," is commonly referenced among medical professionals to reflect the utmost importance placed on patient care. The phrase is often attributed to the original version of the Hippocratic oath, though its true derivation is, in fact, unknown.

Regardless of the etymology, the sentiment is clear: above all else, a healthcare professional should consider patients' well-being. And in 2019, "well-being" has evolved to include privacy and cybersecurity concerns.

Healthcare organizations are increasingly being targeted by cyberattacks due to the gold mine of personal data they possess. The potential, real-world effect these attacks can have is substantial. (See the WannaCry and NotPetya ransomware attacks of 2017.)

Cyberattackers now have the ability to access, steal and sell patient information on the dark web. Beyond that, they have the ability to shut down a hospital's access to critical systems and patient records, making effective patient care virtually impossible.

And, with increased adoption of medical and IoT devices, the surface area for healthcare attacks is becoming even larger. The problem has been further compounded by limited cybersecurity staffing and stagnant cybersecurity budgets in the industry.

The silver lining has been that awareness of the problem has never been higher. While the industry has traditionally lagged when compared with, say, finance or retail, the healthcare ransomware attacks of 2017 (and the many others to follow) served as a clarion call that too many cyberattackers do not adhere to the principle of "do no harm."

In this seminal report on the state of cybersecurity in the healthcare industry, **Carbon Black collaborated with 20 of the industry's leading CISOs to determine how attackers have evolved over the past year,** the biggest concern these security leaders have (HINT: it's not cybersecurity for most) and how confident they are in their cybersecurity programs. This report is a companion piece to the popular "Modern Bank Heists" report from Carbon Black, which reported on the state of the finance industry in March of 2019.

We would like to thank the numerous healthcare security leaders who participated in this report as well as several individuals who added valuable insights: Brian Gladstein, Ryan Murphy and Patrick Upatham.

TOO MANY CYBERATTACKERS DO NOT ADHERE TO THE PRINCIPLE OF **"DO NO HARM."**

Carbon Black.

Key Report Findings

1. **83% of surveyed healthcare organizations** said they've seen an increase in cyberattacks over the past year

2. In 2018, **Carbon Black's healthcare customers saw an average of 8.2 attempted cyberattacks per endpoint each month** according to Carbon Black's data

3. **Two-thirds (66%) of surveyed healthcare organizations** said cyberattacks have become more sophisticated over the past year

4. **Nearly half (45%) of surveyed healthcare organizations** said they've encountered attacks where the primary motivation was **destruction of data** over the past year

5. **One-third (33%) of surveyed healthcare organizations said they've encountered instances of island hopping** on their enterprises over the past year

6. **One-third (33%) of surveyed healthcare organizations said they've encountered counter incident response** over the past year

7. Malicious Microsoft Office documents, most notably **Excel documents with macro-enabled PowerShell delivery cradles,** have been the most common fileless attack method targeting Carbon Black's healthcare customers over the past year, according to Carbon Black's data

8. **Two-thirds (66%) of surveyed healthcare organizations** said their organization was targeted by a ransomware attack during the past year

9. When asked, **"What is the biggest concern to your organization?"** the top answers in our survey were: compliance (33%), budget & resource restrictions (22%), loss of patient data (16%), vulnerable devices (16%), and inability to access patient data (13%)

10. **84% of surveyed healthcare organizations said they train their employees on cybersecurity best practices** at least once per year. Nearly half **(45%) said they conduct training multiple times per year** for employees

11. When asked to self-grade their organization's cybersecurity posture, the top three answers were: **C (33%), B (25%) and B- (16%)**

12. The hottest dark web marketplace listings for healthcare-related information include: **provider data, forgeries, and hacked health insurance company login information**

Attack Frequency

According to our survey, **83% of healthcare organizations** said they've seen an increase in cyberattacks over the past year. This number is not only congruent to industry data we've seen but also aligns with conversations we have with CISOs around the world. Invariably, when we talk to these CISOs, almost all of them are saying that the number of relevant and actionable security alerts they are receiving continues to climb year over year.

When we looked at attack data regarding Carbon Black healthcare customers specifically, the **average endpoint saw 8.2 attempted attacks per month,** as indicated by an actionable alert score greater than six inside Carbon Black's cloud endpoint protection platform (EPP).

Carbon Black.

INCREASE OR DECREASE IN ATTACKS OVER THE PAST YEAR?

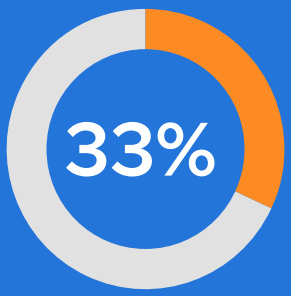
INCREASE IN ATTACKS NO INCREASE IN ATTACKS

Attack Sophistication & Types

Two-thirds (66%) of surveyed healthcare organizations said cyberattacks have become more sophisticated over the past year.

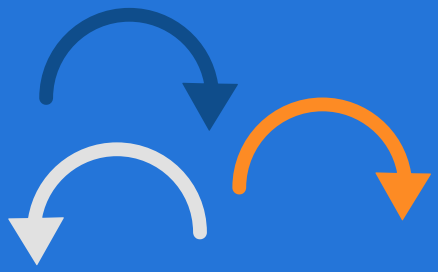
This sophistication is taking multiple forms including destructive attacks, island hopping, counter incident response and fileless attacks.

According to our survey, **nearly half (45%) of healthcare organizations** said they've encountered attacks where the primary motivation was **destruction of data** over the past year. **One-third (33%) of surveyed healthcare organizations said they've encountered instances of island hopping** on their enterprises over the past year. Secondary infections abound in the healthcare sector.



33% OF SURVEYED HEALTHCARE INSTITUTIONS ENCOUNTERED ISLAND HOPPING

Carbon Black.



Island hopping is propagated via three methods:

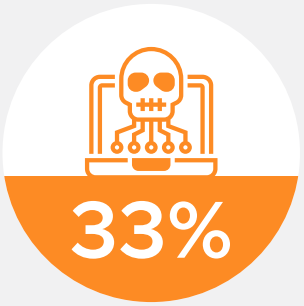
- Network attacks
- Watering-hole attacks
- Reverse business email compromise (BEC)

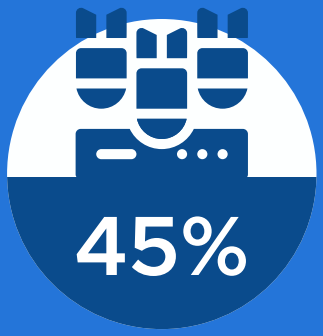
Island hopping attacks come from a wide variety of vantage points, whether it's through partner provisioned Virtual Desktop Infrastructure (VDI) access, private network links and VPNs or by leveraging the compromise of partners to establish trust and perform trusted social engineering attacks. In the case of reverse BEC, a cybercriminal commandeers a mail server and then conducts whaling by sending email with fileless malware. The end result of all of these attacks is the risk of a long-term hostage siege, with the attacker setting up command posts throughout the network. This method allows the cybercriminal to contaminate the hospital network turning the hospital's digital brand into "patient zero". Frequent threat hunting is a critical requirement to identify and mitigate these transient and obfuscated points of presence.

One-third (33%) of surveyed healthcare organizations said they've encountered counter incident response over the past year.

33% OF SURVEYED HEALTHCARE ORGANIZATIONS REPORTED EXPERIENCING COUNTER INCIDENT RESPONSE

Carbon Black.





45% OF SURVEYED HEALTHCARE ORGANIZATIONS REPORTED ENCOUNTERING **DESTRUCTIVE ATTACKS OVER THE PAST YEAR**

Carbon Black.

With counter incident response, attackers are increasingly fighting back to protect their position. Rather than just avoid detection, they are taking counter-measures to thwart responders and maintain their presence throughout the network.

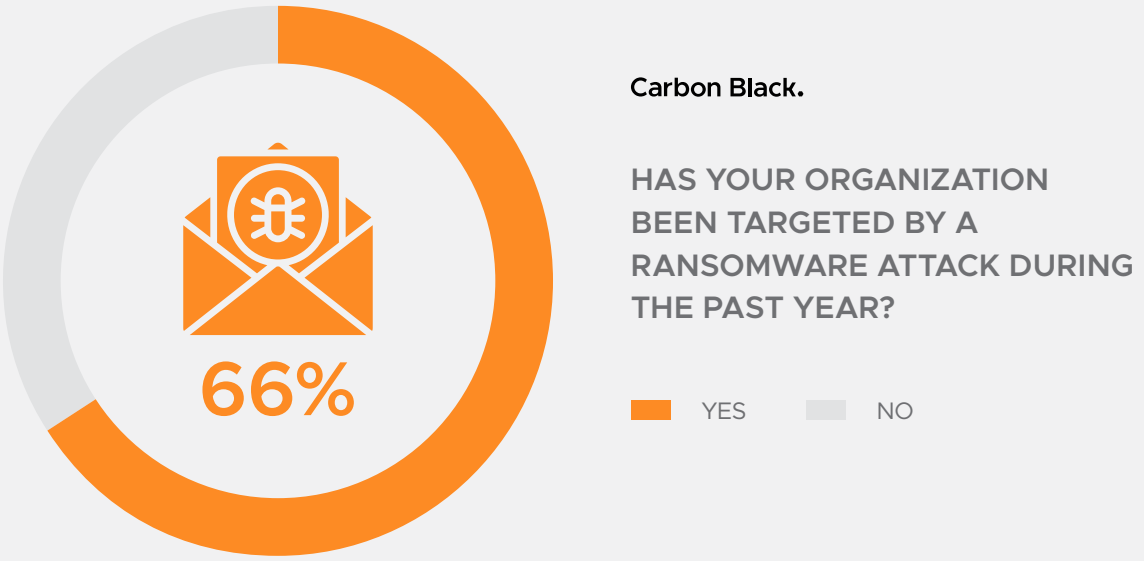
Destructive attacks are tailored to specific targets, cause system outages and destroy data in ways designed to paralyze an organization's operations. These attackers aren't just committing simple burglary or even home invasion — they're arsonists. These attacks are often carried out by punitive and malicious nation-states, including Russia, China and North Korea.

When it comes to fileless attacks and healthcare, we dug into our own customer attack data and found that the most common form of fileless attack our healthcare customers encountered over the past year has been via **Excel spreadsheets with macro-enabled PowerShell delivery cradles.** Ever since the Dridex malware campaign of 2011, malicious macros have become a staple ammunition for hackers who want to bypass legacy antivirus (AV).

Ransomware

It's impossible to discuss cyberattacks in the healthcare industry without referencing ransomware. Though the threat of ransomware has quieted down (at least publicly) since the days of WannaCry and NotPetya, the threat is still very real.

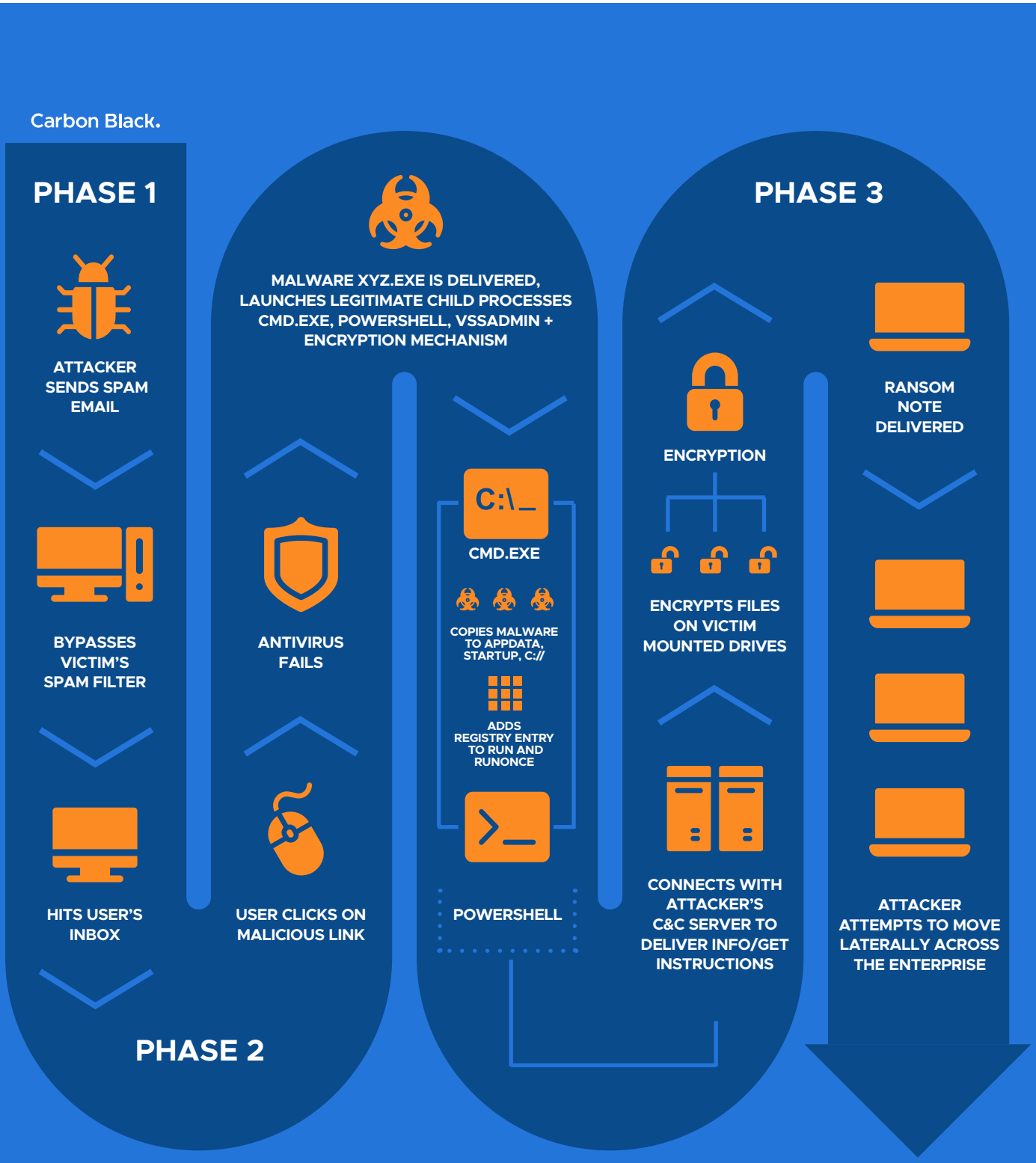
According to our survey, **two-thirds (66%) of healthcare organizations** said their organization was targeted by a ransomware attack during the past year.



Ransomware in healthcare is a dangerous game. In targeting healthcare organizations, ransomware attackers are taking advantage of the "do no harm" principle. Meaning, when forced to decide between paying a ransom or being unable to access critical patient files, the healthcare provider has no choice - they have to pay, lest a patient potentially incur great harm or loss of life. Let us not forget when Medstar hospitals in Washington D.C., were crippled by ransomware three years ago. Patients had to be pulled off operating room tables while in surgery and all new patients were diverted to Maryland and Virginia.

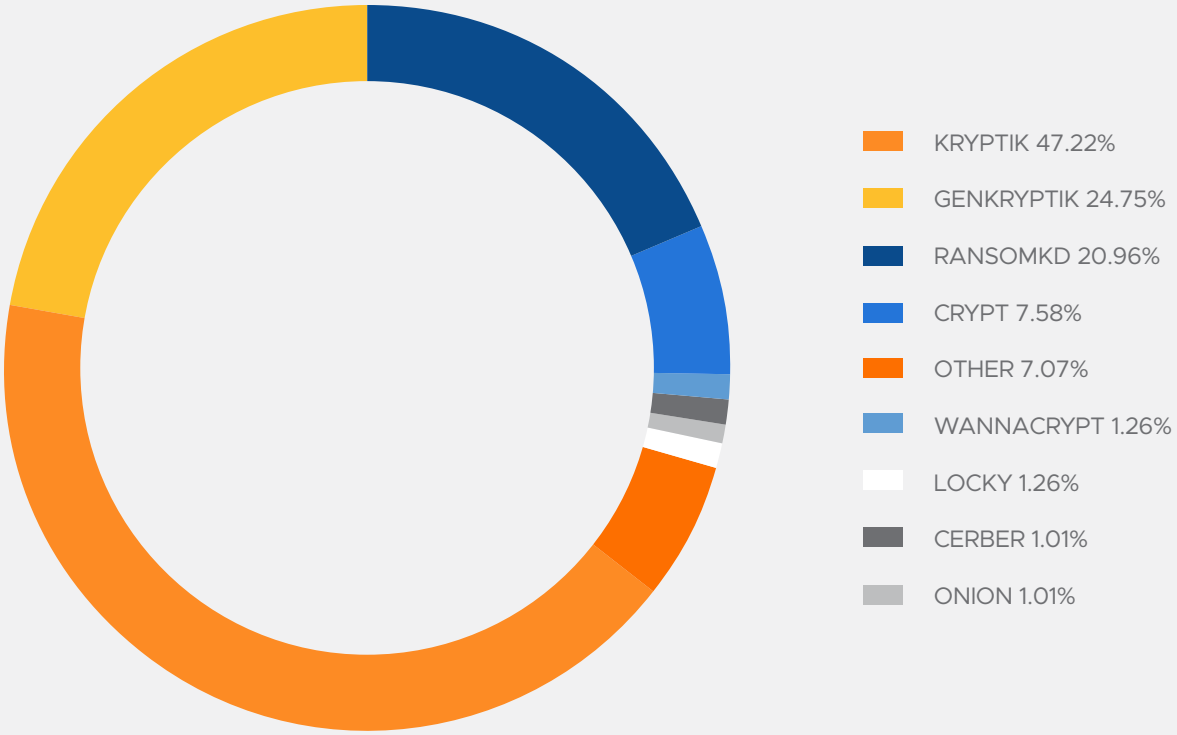
And, for ransomware authors, successful creation and selling of ransomware offerings appears to be fruitful. Based on some of our earlier research, some ransomware sellers are making more than $100,000 per year simply retailing ransomware. In some instances, this is double the salary for legitimate software developers, who pull in an average of $69,000 a year, according to PayScale.com. (In Eastern Europe developer salaries are a bit lower, hovering around $45,000.)

Anatomy of a Ransomware Attack



Carbon Black.

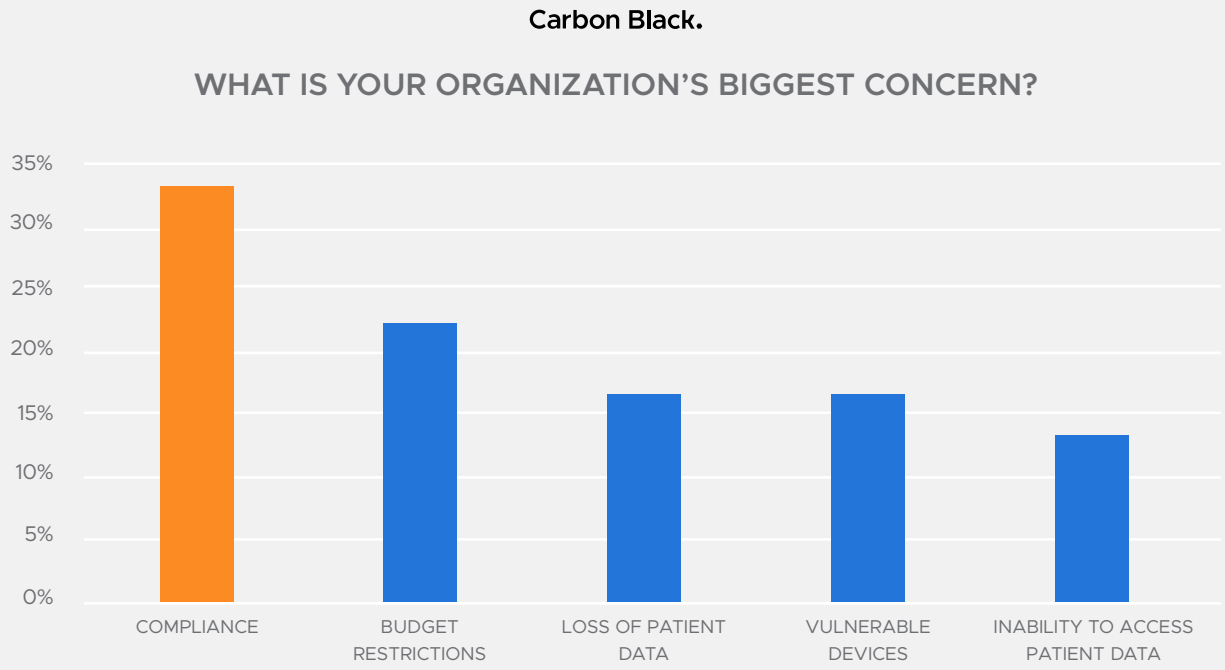
MOST PREVALENT RANSOMWARE VARIANTS TARGETING HEALTHCARE CUSTOMERS IN 2018



According to our own attack data, **Kyptik was the most prevalent ransomware variant** targeting Carbon Black healthcare customers in 2018 followed by GenKryptik and RansomKD.

Compliance, Employee Training, Threat Hunting & Making the Grade

When asked, **"What is the biggest concern to your organization?"** the top answers from CISOs were: compliance (33%), budget & resource restrictions (22%), loss of patient data (16%), vulnerable devices (16%), and inability to access patient data (13%).



This particular data point reflects what is, perhaps, one of the biggest issues in healthcare security. As is often said by leading security minds: "compliance does not equal security." Too many healthcare organizations that were "compliant" ended up becoming breach victims. It's concerning that "compliance" was the top answer to this survey question.

Approaching security with a "checkbox" mentality opens the door for building a security program that covers the bare minimum for data protection. While improvements are continuously being made to compliance standards, a security program should be built to meet the specific needs of an organization. Compliance standards are a great starting point, but should not be considered a dogmatic blueprint for building effective security. We hope to see this number shift is future surveys.

84% OF HEALTHCARE ORGANIZATIONS SAID THEY TRAIN THEIR EMPLOYEES ON CYBERSECURITY BEST PRACTICES AT LEAST ONCE PER YEAR

Carbon Black.

When it comes to cybersecurity in healthcare, education and employee awareness are often critical. We were encouraged to see that **84% of healthcare organizations said they train their employees on cybersecurity best practices at least once per year. Nearly half (45%) said they conduct training multiple times per year** for employees.

Only one-third of healthcare organizations said they currently have a threat hunting team.

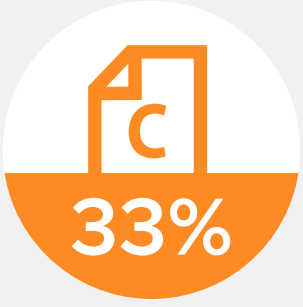
It's no longer realistic to base security strategy on reactive defense alone. The inevitability of breach puts pressure on organizations to start proactively detecting and neutralizing attack vectors by improving visibility, hunting threats and developing effective measures to combat counter incident response. In recent surveys around the globe, the vast majority of CISOs reported that threat hunting significantly improved their overall security posture. Threat hunting is also no longer an activity reserved for the security elite. Modern and easy-to-use threat hunting software is helping businesses of all sizes gain visibility across their businesses. This is a number we hope to see rise in future surveys.

When asked to self-grade their organization's cybersecurity posture, the top three answers from healthcare CISOs were: **C (33%), B (25%) and B- (16%).**

C WAS THE LETTER GRADE

MOST OFTEN GIVEN (33%) BY CISOS ASKED TO GRADE THEIR ORGANIZATION'S CYBERSECURITY POSTURE

Carbon Black.



The Dark Web's Role in Healthcare Cybercrime

Recent analysis of offerings on the dark web following the closure of the largest marketplace, Wall Street Market (WSM), indicates that valuable data from the healthcare industry exceeds protected health information (PHI) data and the hottest offerings today are provider data, forgeries, and hacked health insurance company login information.

Recently, German authorities shut down one of the largest dark web markets, Wall Street Market (Dream Market shut itself down at the end of April.) These markets held a treasure trove of stolen data, including healthcare records. A lack of PHI data on the remaining markets is likely temporary, and healthcare records and data will resurface on different markets or reincarnations of the shuttered markets.

Hackers may even repackage the data in other "fullz" listings. Hackers rely on the fluid nature of dark web markets to remain anonymous and to stay ahead of the authorities.

Current Healthcare Dark Web Offerings

Provider Data

The most expensive and quite alarming, based on the listing descriptions. The listings offer all the documents needed to pose as a medical doctor, including: malpractice insurance documents, medical diplomas, board recommendations, medical doctor licenses, and DEA licenses. Cost per listing is $500.

Forgeries

Forgeries are more numerous and are cheaper than provider data (Between $10 and $120 per record). They take the form of forged prescription labels/sales receipts and forged/stolen/scanned healthcare cards.

Hacked Health Insurance Login Information

Hacked health insurance login information is far less expensive. Less than $3.25 per record on average.

HACKERS RELY ON THE FLUID NATURE OF DARK WEB MARKETS TO REMAIN ANONYMOUS AND TO STAY AHEAD OF THE AUTHORITIES.

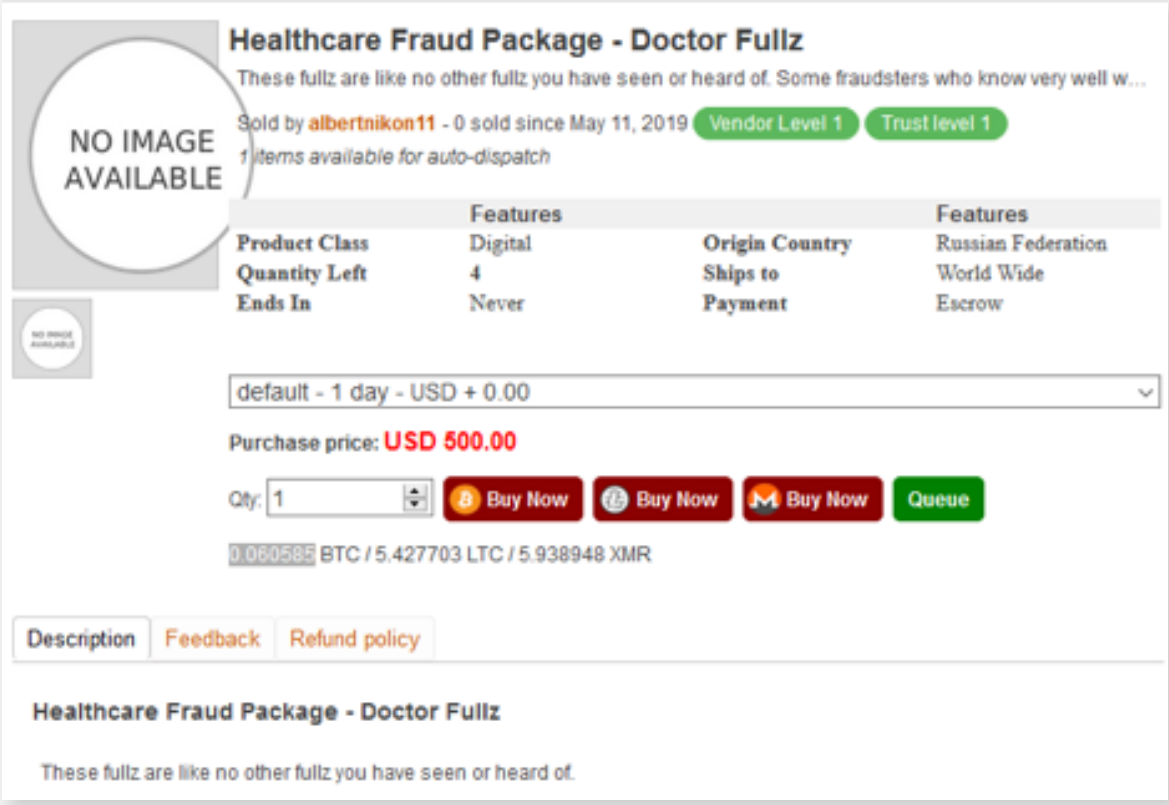
Carbon Black.

Monetizing Medical Information

1

Hacked Provider Data

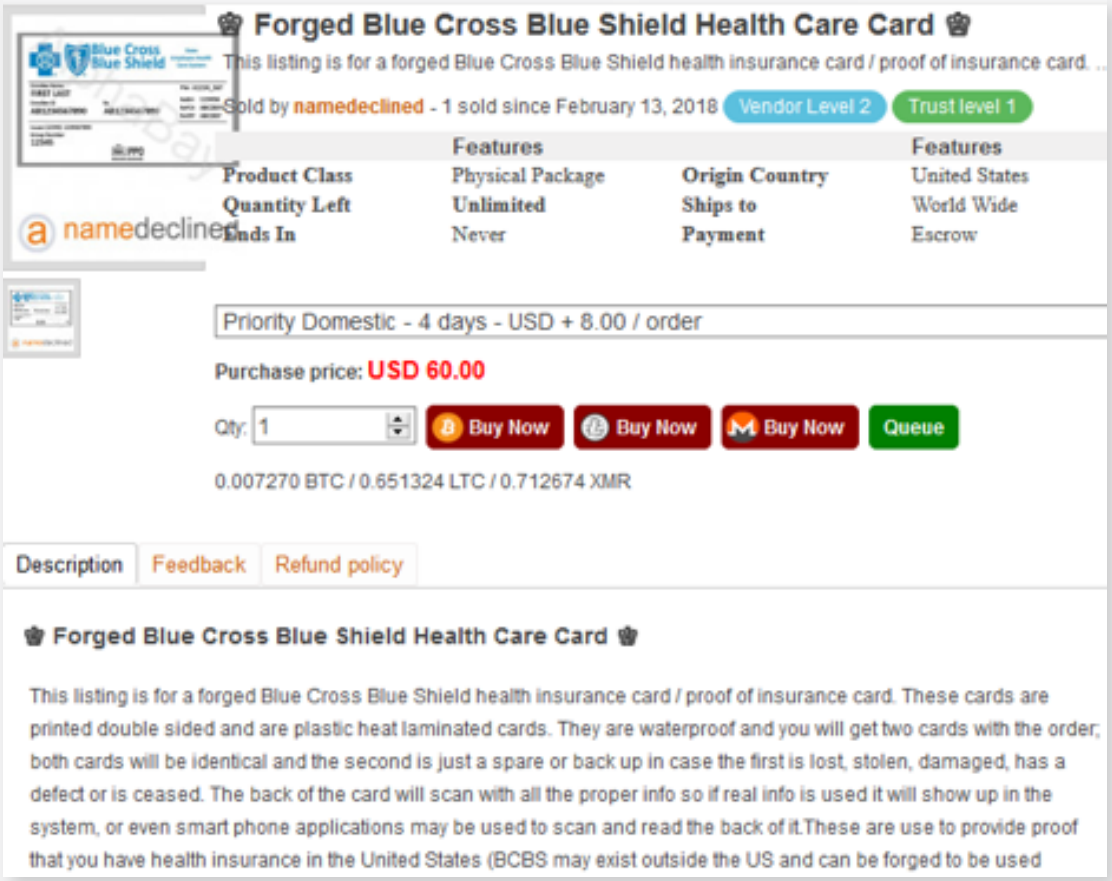
A hacker compromises the corporate network of a healthcare provider to find administrative paperwork that would support a forged doctor's identity. The hacker then sells to a buyer or intermediary (who then sells to the buyer) for a high enough price to ensure a return on investment but low enough to ensure multiple people buy the item. The buyer poses as the stolen doctor's identity and submits claims to Medicare or other medical insurance providers for high-end surgeries.



2

Hacked Health Insurance Login Information

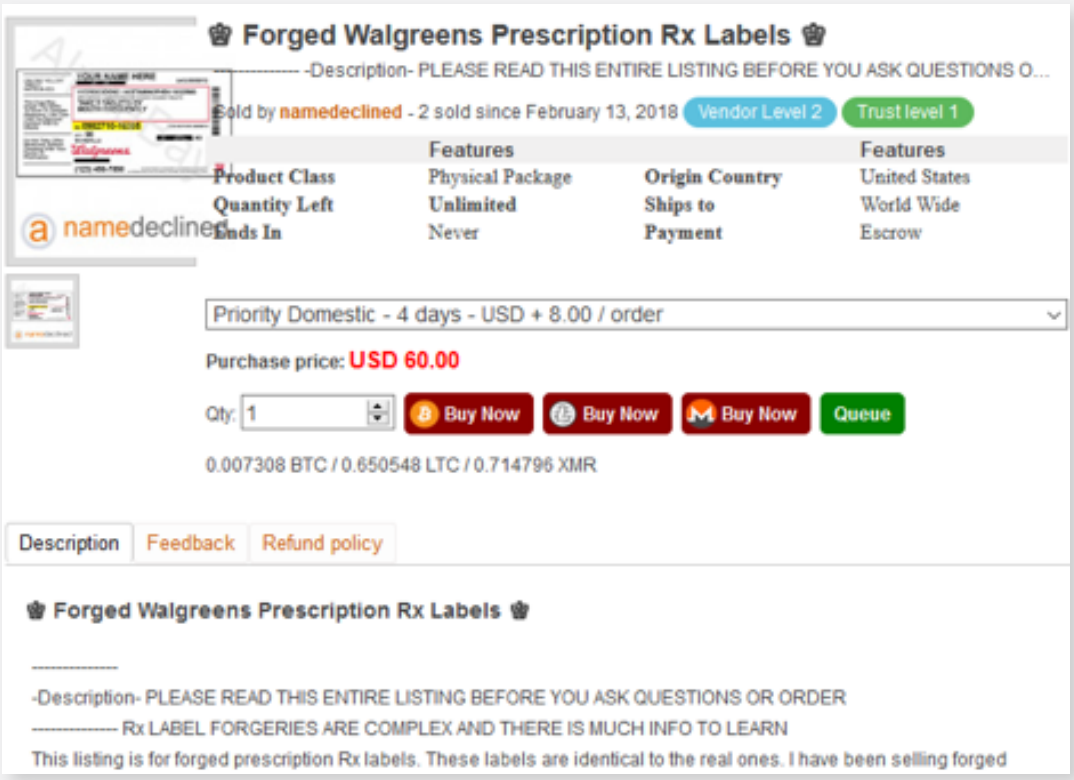
A hacker compromises a web server or credential database. The hacker then sells to a buyer for a low price due to the speed with which the login credentials can change after the compromise is discovered. The buyer uses the login information to gain access to actual medical insurance information, possibly to be combined with the forgery listings. The buyer then uses forged medical information to obtain services at the cost of the victim.



3

Forged Prescription Labels

The seller is provided the critical information to make the customized prescription label for the buyer. The buyer then uses the fake prescription label as a defense against positive drug tests and when carrying drugs through the airport.



4

Personal Health Information

PHI is worth three times as much as PII due to the reality that it is permanent and can never be changed. Hacked PHI can be used by nation states against individuals who have health issues as a method of extortion or compromise.

Security Recommendations for Healthcare CISOs

Based on the data gathered for this report, Carbon Black has a set of recommendations for CISOs in the healthcare industry:

1. **Increase endpoint visibility.** With the growing sophistication of attacks, CISOs need to look at any connected asset as a potential target. This includes electronic medical-record systems, medical devices, payment processing systems, and more.

2. **Establish protection from emerging attacks.** With the potential attack surface growing and evolving quickly, you need to stop as much as possible. This means leveraging a variety of technologies from whitelisting to streaming analytics to behavioral prevention.

3. **Run automated compliance and vulnerability assessments.** With the risk of island hopping ever present, you should be auditing systems regularly and establishing remediation steps across all your security infrastructure.

4. **Work with healthcare-focused MDRs if needed.** There are a variety of managed detection & response service providers out there who specialize in the unique challenges faced by healthcare organizations. When resources are short, these shops can quickly improve your security posture.

5. **As always, backup your data.** Destructive attacks, including ransomware, don't need to destroy your business. Employ best practices for data backup to ensure your data is never at risk.

Conclusion

In healthcare, prevention often stands to be the best cure. This holds true for both physical and digital health. A person's digital (and often physical) health can be directly tied to the cybersecurity posture of their healthcare providers. And, for these healthcare providers, it appears some progress is being made. Regular education of employees, greater awareness of modern threats and the prospect of building out larger threat hunting teams can all go a long way in helping to curb attacks. As we've learned from this survey of some of the world's leading healthcare CISOs, it does not appear that the volume and frequency of attacks will be abating anytime soon. Extreme vigilance among these security teams will be required to help stem the tide in 2019 and beyond.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leader in cloud endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint protection and IT operations into an extensible cloud platform that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 5,300 global customers, including 35 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com