the GORILLA GUIDE® to...

Ransomware for Healthcare

How Best To Defend Yourself Against Ransomware

KATHERINE GORHAM

CROWDSTRIKE | DLT A TECH DATA COMPANY

POWERED BY ActualTech MEDIA

THE GORILLA GUIDE TO...®

Ransomware for Healthcare

Express Edition

By Katherine Gorham

ACTUALTECH MEDIA

6650 Rivers Ave Ste 105 #22489
North Charleston, SC 29406-4829
www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

EDITORIAL DIRECTOR

Keith Ward

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

CREATIVE DIRECTOR

Olivia Thomson

SENIOR DIRECTOR OF CONTENT

Katie Mohr

PARTNER AND VP OF CONTENT

James Green

WITH SPECIAL CONTRIBUTIONS FROM CROWDSTRIKE

Kurt Baker

Grace Bergen

Drex DeFord

Todd Felker

Bart Lenaerts-Bergmans

Andrew Matthews

Nina Padavil

ABOUT THE AUTHOR

Katherine Gorham is a writer and editor with a focus on information security. She excels at information synthesis and can truly understand how all the pieces of complex modern information systems fit together … and how they can be vulnerable to attack.

ENTERING THE JUNGLE

Introduction 7

Chapter 1: The Crime That Keeps Changing 9

- A Short History of Ransomware 10
- When It's Not Just About the Money 13
- Know Your Enemy 16

Chapter 2: The World of Cybercrime 17

- Getting Into Your Network 18
- The Patching Dilemma 19
- Moving Laterally 22
- The Rise of Big Game Hunting 24

Chapter 3: Why Crime as a Service? 27

- The Exploit Market 30

Chapter 4: The Ransom Dilemma 32

- Plan for the Worst 33
- Don't Go It Alone 34

Chapter 5: Defending Yourself Against Ransomware 36

- Defense in Depth 37
- Get Help 37
- Gain Intelligence About the Threats 38

CALLOUTS USED IN THIS BOOK

The Gorilla is the professorial sort that enjoys helping people learn. In the School House callout, you'll gain insight into topics that may be outside the main subject but are still important.

This is a special place where you can learn a bit more about ancillary topics presented in the book.

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

Takes you into the deep, dark depths of a particular topic.

Discusses items of strategic interest to business leaders.

ICONS USED IN THIS BOOK

DEFINITION

Defines a word, phrase, or concept.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

PAY ATTENTION

We want to make sure you see this!

GPS

We'll help you navigate your knowledge to the right place.

WATCH OUT!

Make sure you read this so you don't make a critical error!

TIP

A helpful piece of advice based on what you've read.

INTRODUCTION

Healthcare organizations have seen a dramatic uptick in ransomware attacks since the start of the COVID-19 pandemic. This represents the sharp acceleration of a trend which had seen attacks on this sector grow for many years. Combined with the intense stress on everyone working in this sector due to the pandemic, healthcare organizations are uniquely vulnerable to information security threats such as ransomware.

Any heavily regulated sector tends to become a target for cybercriminals. Government and education, for example, have similar vulnerabilities to healthcare in that there are significantly fewer service providers that serve this vertical. Regulation is difficult to navigate, fewer IT professionals are available that are conversant with sector-specific regulations, and thus it is only economically feasible for a limited number of service providers to serve that space. This makes it important that everyone in the IT decision chain has at least a basic understanding of IT threats and risks.

Healthcare IT — any life-critical IT — has significant additional considerations when compared to other regulated sectors. In addition to mandated regulations, the legal environment of life-critical IT makes vendors that sell into this space extremely risk-averse. Even with this risk aversion, however, a significant number[1] of healthcare sector breaches comes from this sector's IT supply chain.[2]

Many healthcare providers also have a higher-than-average number of Internet of Things (IoT) devices to worry about. Sensors, medical

[1] https://www.scmagazine.com/feature/breach/10-biggest-healthcare-data-breaches-of-2021-impact-over-22-6m-patients

[2] https://www.hcinnovationgroup.com/cybersecurity/data-breaches/article/21209658/with-new-attack-vectors-healthcare-data-breaches-continued-to-soar-in-2020

devices, medical imaging and security systems are all examples of network-connected devices that are often unpatched, unpatchable or simply subject to very long periods between a vulnerability being disclosed and a patch being made available.

Before the pandemic, rationalizing an IT environment that was simultaneously experiencing significant pressure to be risk-averse while also deploying IoT devices at an unmanageable pace was already challenging IT teams. IT teams have been struggling for years with "shadow IoT" devices deployed by non-IT departments. Since the pandemic, these problems have been magnified by a pandemic-driven need to onboard new suppliers (and the IT integration that entails), coupled with staff burnout and retention challenges.

Failure is not an option in healthcare IT, regardless of the spiraling technical debt. For all of these reasons, the healthcare sector is the perfect target for cybercriminals, especially ransomware groups. This Gorilla Guide can help you understand the unique threat that ransomware poses, as well as the ever-evolving criminal ecosystem that has led to an explosion of ransomware in all sectors of our society.

It's full of information you need to defend your organization from these attacks and is focused on the special needs of healthcare organizations. In these pages you'll learn all about ransomware, how it works, why it's expanding and ways to protect your organization from the ravages of this scourge.

If you have operations responsibility for your organization's network, or are a C-level security executive who has to make decisions on spending money to stay safe, this guide is for you. We'll start off with some essential background about ransomware, and how we got to this point.

CHAPTER 1

The Crime That Keeps Changing

Since the first known attack in the late 1980s, ransomware has been constantly evolving. Attackers keep shifting tactics to stay ahead of common defenses, prey on current fears and extract as much money as possible from their victims. How the attack is delivered, what damage it does to the target systems, what the threats are, how much ransom is demanded and how the ransom is paid — these are all subject to constant innovation and change.

The common element to all ransomware is extortion. A ransomware attacker threatens damage, data loss or embarrassing data leaks unless the victim pays them. The motivation for ransomware is usually financial gain — but even that is beginning to change in some cases.

RANSOMWARE

Ransomware is a type of malware attack that involves extortion. It encrypts a victim's data until a payment is made to the attacker. If the ransom payment is not made, the attacker may permanently block access to the victim's data and/or publish their sensitive data on dedicated leak sites (DLS).

Ransomware attacks are pervasive, high-stakes and increasingly expensive. In the 2021 CrowdStrike Global Security Attitude Survey,[3] 66% of respondents reported that their organization had suffered a ransomware attack in the last 12 months, with similarly alarming numbers reported elsewhere.

A Short History of Ransomware

One of the earliest examples of ransomware was the PC Cyborg Virus (also known as the AIDS Trojan) in the late 1980s (see **Figure 1**). It was delivered via floppy disk and locked victims out of their computers until they sent money to the attacker via mail.

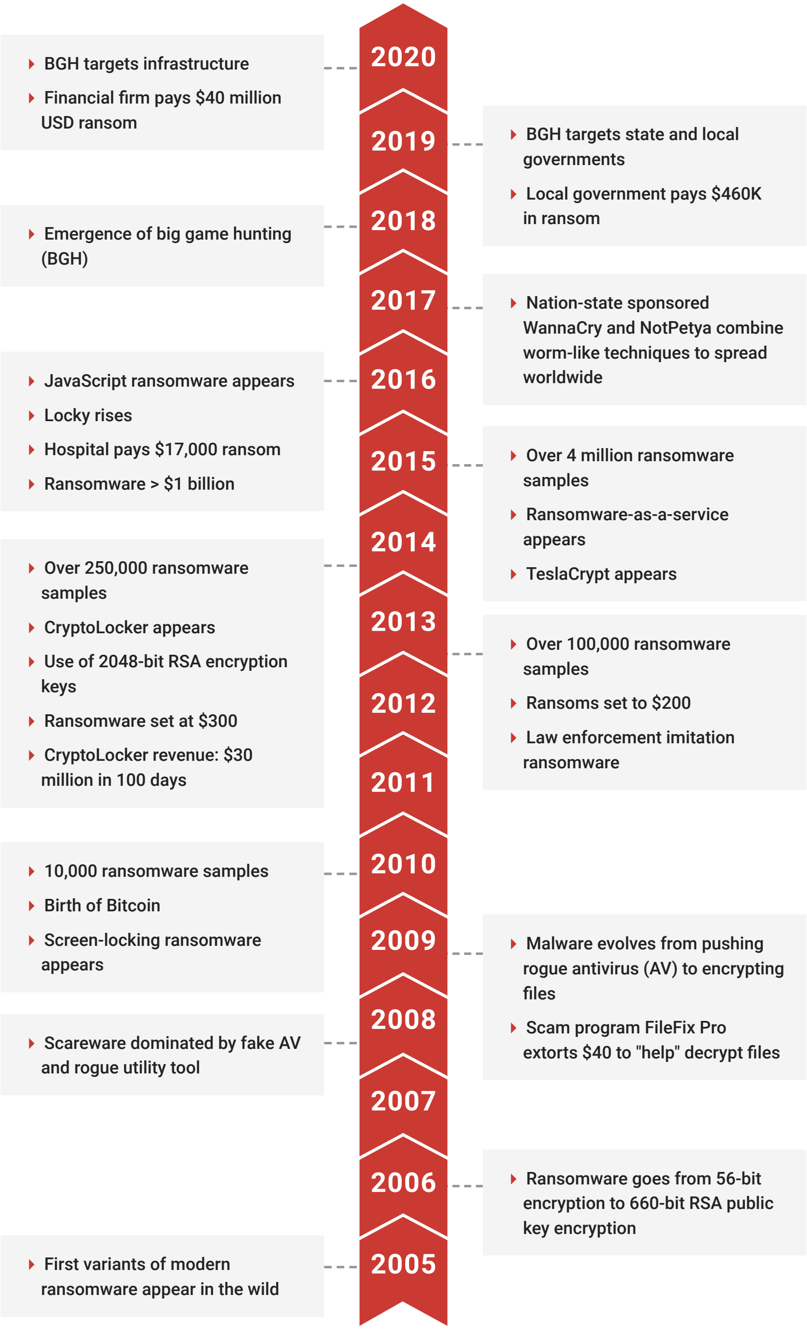
Another early ransomware type was "scareware," which showed victims alarming pop-up messages stating that they had been infected by a computer virus and urging them to download an "antivirus" program to fix the problem.

Ransomware was not terribly popular among criminals at first, perhaps because it was difficult to get the ransom money in a way that was not easily traced by law enforcement. However, this changed in 2010 with the advent of Bitcoin and other cryptocurrencies. Now criminals could collect ransom in a much more anonymous way, and ransomware exploded in popularity.

Bitcoin simplified ransom collection for criminals, but it had a steep learning curve for victims. To expedite payment, some attackers started offering detailed instructions on how to buy and transfer Bitcoin — in essence, providing tech support for victims. This foreshadowed the development of the "as a service" eCrime ecosystem.

Within the U.S. healthcare sector, one of the first well-publicized attacks occurred in 2016, when the Hollywood Presbyterian Medical Center experienced a ransomware incident for which it paid $17,000

[3] https://www.crowdstrike.com/blog/2021-crowdstrike-global-security-attitude-survey/



2020

- BGH targets infrastructure
- Financial firm pays $40 million USD ransom

2019

- BGH targets state and local governments
- Local government pays $460K in ransom

2018

- Emergence of big game hunting (BGH)

2017

- Nation-state sponsored WannaCry and NotPetya combine worm-like techniques to spread worldwide

2016

- JavaScript ransomware appears
- Locky rises
- Hospital pays $17,000 ransom
- Ransomware > $1 billion

2015

- Over 4 million ransomware samples
- Ransomware-as-a-service appears
- TeslaCrypt appears

2014

- Over 250,000 ransomware samples
- CryptoLocker appears
- Use of 2048-bit RSA encryption keys
- Ransomware set at $300
- CryptoLocker revenue: $30 million in 100 days

2013

- Over 100,000 ransomware samples
- Ransoms set to $200
- Law enforcement imitation ransomware

2012

2011

2010

- 10,000 ransomware samples
- Birth of Bitcoin
- Screen-locking ransomware appears

2009

- Malware evolves from pushing rogue antivirus (AV) to encrypting files
- Scam program FileFix Pro extorts $40 to "help" decrypt files

2008

- Scareware dominated by fake AV and rogue utility tool

2007

2006

- Ransomware goes from 56-bit encryption to 660-bit RSA public key encryption

2005

- First variants of modern ransomware appear in the wild

Figure 1: Ransomware Timeline

USD in ransom. By today's standards this is a positively quaint ransom payment, but it was a notable amount for the day.

By 2021, ransomware demands were much higher, with CNA Financial Corp. in the United States paying out over $40 million USD[4], with an average worldwide cost of $9.23 million USD.[5] In 2021 the top 10 breaches in the United States alone accounted for the compromise of over 22.6 million patient records.[6]

Ransomware is pervasive throughout multiple sectors, and throughout the world with the non-monetary effects of ransomware attacks becoming even more apparent. Attacks on meat-processing companies,[7] for example, have affected the availability and price of groceries.

Ransomware can impact organizations in unexpected ways. The Colonial Pipeline attack in May 2021[8] caused fuel shortages in a number of U.S. states and caused many politicians and corporate leaders to reassess the severity of the risk that ransomware poses.

The Colonial Pipeline attack didn't compromise the operational technology (OT) network, which controls the ability of the pipeline to physically function. Unfortunately, however, Colonial Pipeline's operations were still disrupted because the company's billing system (located on the IT network) was compromised.

While the real-world need for integration between IT and OT networks allowed ransomware to render infrastructure critical to a significant portion of the United States inoperable, without ever breaching the OT network itself, the inability of attackers to compromise the OT network demonstrates the increasing criticality of network

[4] https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

[5] https://www.beckershospitalreview.com/cybersecurity/9-2m-is-average-cost-of-a-healthcare-data-breach-ibm-says.html

[6] https://www.scmagazine.com/feature/breach/10-biggest-healthcare-data-breaches-of-2021-impact-over-22-6m-patients

[7] https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html

[8] https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

segmentation and separation. Given the number of vulnerable devices that healthcare providers have to manage, network segmentation is often all that stands between attackers and unpatchable life-critical devices once they have a foothold in your network.

These ransomware events, combined with the 2020 SolarWinds attack[9] (which showed the world how high-impact software supply chain attacks can be) resulted in a response that itself is part of ransomware's history: U.S. President Joe Biden issued an open letter[10] and an executive order.[11] These documents detail new security requirements for U.S. federal government departments and contractors, as well as the creation of the Cybersecurity Safety Review Board, which is modeled after the National Transportation Safety Board. Several other nations are responding in similar fashion.

When It's Not Just About the Money

Not all organizations are equally likely to be impacted by ransomware. Organizations with fewer information security resources — or significant constraints on their IT architectures — are significantly more likely to be impacted. Complicating matters is that law enforcement agencies do not have the resources to investigate every cybercrime.

Estimates in 2019 from the Third Way think tank suggest that as few as 3 out of every 1,000 reported cybercrimes are prosecuted.[12] But due to under-reporting, some experts estimate that the ratio could be as low as 3 in 100,000.[13]

[9] https://arstechnica.com/information-technology/2020/12/18000-organizations-downloaded-backdoor-planted-by-cozy-bear-hackers/

[10] https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf

[11] https://www.crowdstrike.com/blog/what-the-new-cybersecurity-executive-order-means-for-public-sector/

[12] https://www.thirdway.org/report/cyber-enforcement-in-four-key-states

[13] https://www.theregister.com/2020/01/30/cops_crime_failure/

Governments, healthcare providers, and education facilities are frequent victims. By 2020, approximately one-third of all health trusts in the United Kingdom reported being impacted by ransomware.[14] A 2021 survey of 597 health delivery organizations had 42% of respondents indicated they had been hit by *at least two* ransomware attacks in the past two years, while 71% of respondents indicated that the ransomware attacks resulted in longer stays for patients, and 65% said attacks resulted in increased patient transfers to other facilities.[15] That's bad for everybody.

According to the 2021 CrowdStrike Global Security Attitude Survey, 24% of ransomware victims paid the ransom, and those ransoms are getting bigger. In March 2021, a ransom demand of $50 million USD was made to tech giant Acer — the highest publicly known ransomware demand at the time of writing.

Ransoms, however, are only part of the cost. For example, Universal Health Services (UHS), which operates more than 400 U.S. and U.K. healthcare facilities, estimates the impact of the September 2020 Ryuk ransomware attack at $67 million USD.[16]

And the non-monetary impacts are beginning to be felt, with ransomware affecting the availability of food, fuel, water and the delivery of medical care. Consider 2019, when 764 healthcare organizations temporarily ceased operations because of ransomware in the United States alone.[17] By 2020, a separate organization noted 560 healthcare organizations in the United States were impacted.[18]

In healthcare, more than any other sector, ransomware is about more than just money. Lives truly are demonstrably at risk from this threat.

[14] https://www.infosecurity-magazine.com/news/local-government-targeted/

[15] https://www.censinet.com/ponemon-report-covid-impact-ransomware

[16] https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

[17] https://pentestmag.com/ransomware-statistics-trends-and-facts-for-2020-and-beyond/

[18] https://www.beckershospitalreview.com/cybersecurity/ransomware-attacks-cost-healthcare-orgs-20-8b-in-2020.html

HEALTHCARE, SCHOOLS AND GOVERNMENTS ARE ATTRACTIVE TARGETS

According to *The Washington Post*, more than 2,000 local governments, healthcare facilities, and schools were victims of ransomware attacks in 2020.[1] These organizations often have smaller IT departments with limited budgets for cybersecurity, making them appealing to attackers.

[1] https://www.washingtonpost.com/local/local-government-ransomware-dc/2021/08/05/048051cc-efc6-11eb-81d2-ffae0f931b8f_story.html

High-profile organizations are often the target of state-sponsored attackers as well as commercial criminals looking for quick cash, and the line between the two types of attackers can at times be blurry.

Governments and large corporations, as well as healthcare and education providers in particular, are frequently targeted by hacktivists trying to make a statement. Attackers may also use cyberattacks — including ransomware — as an attempted market manipulation, or as a cover for data theft and intelligence gathering.

Healthcare in particular is vulnerable to an unthinkable, but very real threat: state actors wishing to damage geopolitical rivals by crippling their healthcare capabilities. Watching the COVID-19 pandemic accomplish this without outside interference has raised awareness of how successful a geopolitical tool this can be, raising the stakes for healthcare organizations immeasurably.

Know Your Enemy

The complexity of the various technologies involved, as well as the varying motivations of attackers, makes threat intelligence a vital part of defenses for all high-profile organizations.

Knowing your enemy is important, because understanding the motivations and methods of attackers leads to better decisions, especially during a crisis.

THREAT INTELLIGENCE

Threat intelligence is data that's collected, processed and analyzed to understand a threat actor's motives, targets and attack behaviors.

Threat intelligence helps us understand attackers and make faster, data-backed security decisions.

Unfortunately, few organizations have the capability to build in-house threat intelligence capabilities. Even with unlimited funding available, there simply aren't enough information security experts for each high-profile organization to build out their own cybersecurity center of excellence.

The industry response to the shortage of expertise has been to build information security tools and threat intelligence services. Not only does this share expertise and capabilities across both public and private domains, but the consultative model allows for lessons learned at one organization to be generalized and applied to others.

CHAPTER 2

The World of Cybercrime

Ransomware is written by software developers whose daily life and concerns are much the same as anyone else's. Today, the development and distribution of criminal malware mirrors the development and distribution of legal software.

Ransomware is only one part of a diverse criminal ecosystem. The same pressures that drove specialization in the legal software world have driven specialization throughout the criminal malware supply chain, up to and including the provisioning of malware functionality as a service.

There are software vendors who write and support the ransomware itself, while other software vendors create the malware (phishing kits) that initially penetrates networks. Access brokers sell access to the networks they've compromised, and various other intermediaries are often involved.

Those who actually deploy the ransomware are frequently groups who specialize in money laundering. Writing malware is hard, and getting targets to execute said malware is even harder. But "following the money" is usually how law enforcement catches the bad guys.

State actors also appear to specialize, with some nations appearing to have more than a dozen different cyber warfare units. Whether internal to a nation-state's efforts, or as part of organized crime, malware in general — and ransomware in particular — is becoming as easy to use as modern software-as-a-service (SaaS) cloud applications.

Getting Into Your Network

Cybercriminals deploying ransomware get initial access to networks the same way that any other cybercriminals do. They most often use zero-day vulnerabilities, which are weaknesses discovered before the vendor has had a chance to issue software patches.

ZERO-DAY VULNERABILITY

A zero-day vulnerability is an unknown security vulnerability or software flaw that a threat actor can target with malicious code. The term "zero-day" is used because the software vendor was unaware of their software vulnerability, and they've had "zero" days to work on a security patch or an update to fix the issue.

The FORCEDENTRY vulnerability, which allowed customers of NSO group to compromise virtually any Apple device without user participation,[19] is an example of a zero-day. These vulnerabilities tend to get all the press, but they are emphatically *not* what lead to most organizations' compromise.

PHISHING

Phishing is a scam by which an internet user is duped (as by a deceptive email message) into revealing personal or confidential information which the scammer can use illicitly.

[19] https://arstechnica.com/information-technology/2021/09/apple-fixes-imessage-zero-day-exploited-by-pegasus-spyware/

The majority of organizations are compromised via stolen or compromised user credentials, frequently involving phishing. A phishing attack frequently begins with an email that encourages either visiting a compromised or impersonated website, or opening a malicious attachment.

Compromised or impersonated websites are often designed to look identical to real websites, and encourage the victim to enter their credentials just as they would on the real website. A malicious attachment, on the other hand, exploits a vulnerability on the local computer, either through the operating system (OS) or an individual application.

Networks can also be compromised by exploiting a vulnerability in an automated system, such as a network router or a website. As with malicious attachments, this attack vector relies on exploiting an OS or application.

All of these vulnerabilities are significantly exacerbated when staff are burnt out. And healthcare staff around the world are not only burnt out, they've resigned in record numbers due to the stress of the pandemic, resulting in chronic understaffing that has no end in sight. Adding to the burden is that many attackers prefer to attack during weekends and holidays, hoping to strike when IT departments are understaffed and not monitoring software closely.

This stress never stays restricted to one group of employees, either. When healthcare practitioners are burnt out they increase stress on back office staff, including IT teams. For the foreseeable future, healthcare organizations are likely to be more vulnerable to human error than almost any other sector.

The Patching Dilemma

In virtually all cases, network compromise would not have been successful had all known vulnerabilities in existing software been patched. Modern operating systems, as well as applications such as web browsers, limit what a standard user can do explicitly to prevent malicious actors from compromising entire computer systems and/or networks.

The average user's credentials don't have administrative access to network systems, so even if attacks begin with compromised credentials, attackers typically need to exploit a software vulnerability to obtain a "privilege escalation." Whether the attack is against an automated system, or requires a human to perform an action, ransomware attackers need to obtain administrative-level security privileges to encrypt entire systems.

Patching all IT equipment as soon as patches become available would solve the overwhelming majority of current malware attacks, including ransomware, but this is far from a simple proposition.

The relentless progress of digital transformation has left few (if any) aspects of modern healthcare organizations untouched, making the scope of patch testing potentially as large as the entire organization itself. In addition, applying patches takes IT systems and services offline, and introduces its own risks.

THE PATCHING DILEMMA

The patching dilemma balances the need to apply security patches immediately against the business impacts of outages.

A patch is a change in software code. This change can consist of new features, or it can be alterations to an existing feature. Frequently, the purpose of patches is to eliminate a vulnerability.

Fileless Malware Is Harder to Detect

Although some well-known ransomware attacks rely on tricking a victim into executing a file, for example by clicking on an email attachment, that's not the only way that ransomware can spread.

Fileless malware will attack without having to load malicious code onto the target device first, making it harder for many legacy antivirus products to detect. Fileless malware may use stolen credentials and legitimate tools already installed on the target system to carry out the attack.

To detect fileless malware, defenders need to be able to look for indicators of attack (IOAs). IOAs are actions an attacker must perform to carry out their goal, which may be detectable even if no malicious code has been downloaded.[1]

[1] https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ioa-vs-ioc/

Unfortunately, patches have a long history of breaking things. Microsoft's MS14-045 patch (which caused Windows computers to blue-screen) is particularly memorable,[20] while Adobe's final patch for Flash famously disabled the application after Adobe ended support for the product. Combined with legacy (and often unpatchable) applications, the many healthcare organizations carry a significant amount of technical debt.[21]

Most organizations approach the patching dilemma by testing patches before deployment. Testing all aspects of an application is frequently time-consuming and is increasingly complicated by the

[20] https://arstechnica.com/information-technology/2014/08/after-blue-screen-of-death-reports-microsoft-says-to-uninstall-recent-patch/

[21] https://www.medtechdive.com/news/legacy-medical-devices-growing-hacker-threats-create-medtech-cyber-risks/602157/

rise of supply chain attacks. Vendor-managed IT present on healthcare networks is also a point of difficulty, as this frequently requires chasing the vendor in order to get updates deployed.

Supply chain attacks involve compromising the third-party software, libraries and integrations used by software, services and IT infrastructure teams. Just as poisoning a water supply can threaten an entire town, compromising a single popular software library can result in a vulnerability in hundreds of applications used by millions of organizations.

The Solar Winds attacks of 2020 and 2021[22] were a particularly notable string of supply chain attacks. These attacks were serious enough to lead to international discussions by world leaders about ransomware,[23] and were followed by even more sophisticated attacks by the same threat actors.[24]

Complex attacks like this are of particular concern to large organizations. Large organizations often reduce their IT burden by centralizing a number of IT functions, and as a result have code repositories, patch libraries and so forth. These repositories are curated and tested by a central team of specialists, and then consumed by downstream organizations, making supply chain attacks a concern both internally and externally.

Moving Laterally

The patching dilemma is why zero-days are rarely required to compromise an organization. The bad guys don't need some ultra-rare, completely unknown, NSO-group-class, zero-touch vulnerability to breach your network. Somewhere on your network is very likely a device that didn't get a critical patch from three years ago, and that's more than enough to let the compromise begin.

[22] https://arstechnica.com/information-technology/2020/12/russian-hackers-hit-us-government-using-widespread-supply-chain-attack/

[23] https://www.nytimes.com/2021/10/14/us/politics/global-ransomware-meeting.html

[24] https://arstechnica.com/information-technology/2021/12/solarwinds-hackers-have-a-whole-bag-of-new-tricks-for-mass-compromise-attacks/

An attacker's first contact with a network is the point of initial compromise. This could be a malicious attachment someone opens, an out-of-date and publicly exposed unattended service, or an attacker logging in to a system using stolen credentials. If the attacker can see *anything* on your network with the right kind of vulnerability, they can attack that system and establish persistence.

EXPLOIT KIT

An exploit kit is an automated piece of malware that tries to gain access to victims' systems when they unknowingly visit a compromised website. Exploit kits are popular because they require very little technical knowledge to use, making them an integral part of the ransomware-as-a-service ecosystem.

Persistence in this context means that the attacker has managed to gain administrative-level privileges on at least one system on the network and has installed malware that allows the attacker to remotely execute commands on the compromised system. Once persistence is established, badness ensues.

Most compromised networks will be bundled together and access to them sold by access brokers. Attackers who purchase access to networks can then continue to move laterally throughout a network, identifying other vulnerable systems and then breaching them as well (see **Figure 2**).

Compromised systems are used for everything from cryptomining to corporate espionage. These systems allow data to be copied from a network, encrypted and ultimately held for ransom. Indeed, many malware families are now effectively modular crimeware platforms

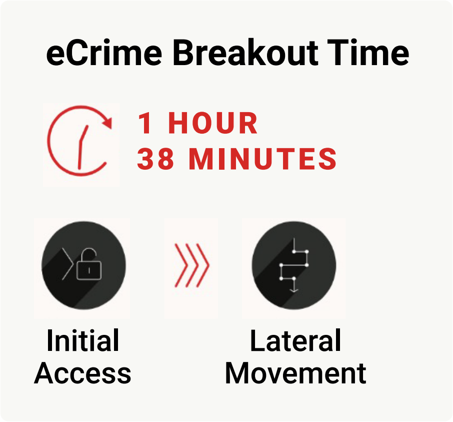


Figure 2: The CrowdStrike 2022 Global Threat Report indicates that average "breakout time" for a threat actor is 1 hour 38 minutes. Breakout time is the time between initial compromise and lateral spread.[25]

that allow anyone who purchases access to a network to quickly install easy-to-use software that allows them to pick from a list of crimes they'd like to commit.[26]

Personal health information (PHI) is of particular interest to attackers, as its value on the dark web is often several times higher than valid credit card numbers. The significant value of PHI to cybercriminals means that even facilities that are not directly practicing patient care (such as medical laboratories) are still tempting targets for threat actors.

The Rise of Big Game Hunting

Just as software vendors in the legal software world specialize in different markets, so too does the criminal malware supply chain. Many access brokers specialize in gaining access to healthcare networks,

[25] https://www.crowdstrike.com/resources/reports/threat-hunting-report-2021/

[26] https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web

while other cybercriminals specialize in moving laterally through healthcare networks.

Healthcare in particular is at risk because of the ongoing specialization of cybercriminals, as well as the significant amount of both IoT devices and on-premises third-party-managed IT. Because of the constricted vendor and service provider space for this sector, many healthcare organizations have similar network architectures, run the same software configured in the same ways and have the same (often unpatched) devices. In one survey, 82% of healthcare organizations had experienced at least one cyberattack directed at IoT devices — an alarming number when talking about only one category of targets in IT.[27]

BIG GAME HUNTING (BGH)

Big game hunting is a ransomware tactic that has seen increased use since 2016.[1] Instead of infecting a large number of targets (e.g., by using the "spray and pray" approach), BGH involves a highly focused and sophisticated attack on a target capable of paying a large ransom.

[1] https://www.crowdstrike.com/blog/ransomware-actors-evolved-operations-in-2020/

Attackers can specialize in compromising these environments, and because they can buy access to multiple networks from access brokers, they can compromise multiple healthcare networks at the same time. This dramatically increases the return on investment for an attacker's time.

The real world of cybercrime is a sophisticated ecosystem with processes, tools, and business relationships similar to the world of

[27] https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-an-iot-cyberattack-in-the-past-18-months/

legitimate software development. This is not good news for defenders. It means that even criminals with relatively little technical knowledge can buy the means to launch a ransomware attack without having to write a single line of code.

Welcome to the era of ransomware as a service: specialized, personalized and persistent (see **Figure 3**).

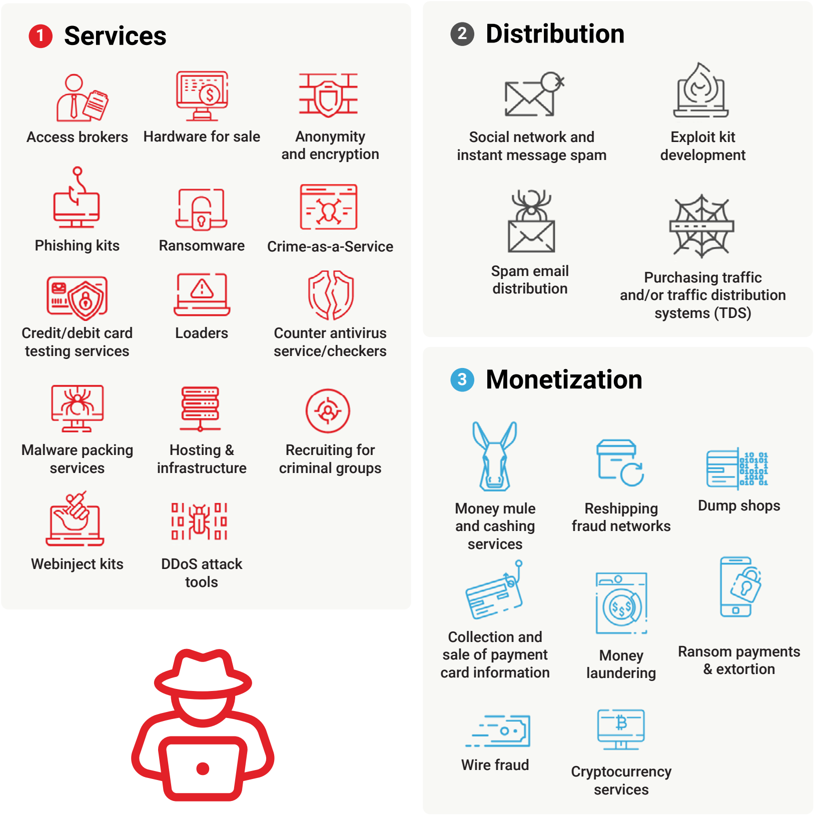

1 Services
Access brokers
Hardware for sale
Anonymity and encryption
Phishing kits
Ransomware
Crime-as-a-Service
Credit/debit card testing services
Loaders
Counter antivirus service/checkers
Malware packing services
Hosting & infrastructure
Recruiting for criminal groups
Webinject kits
DDoS attack tools
2 Distribution
Social network and instant message spam
Exploit kit development
Spam email distribution
Purchasing traffic and/or traffic distribution systems (TDS)
3 Monetization
Money mule and cashing services
Reshipping fraud networks
Dump shops
Collection and sale of payment card information
Money laundering
Ransom payments & extortion
Wire fraud
Cryptocurrency services

Figure 3: Ransomware as a Service[28]

[28] https://www.crowdstrike.com/resources/reports/threat-hunting-report-2021/

CHAPTER 3

Why Crime as a Service?

If television has taught us anything, it’s that getting away with crime gets harder as awareness grows of the criminal activity. A crime-as-a-service ecosystem is, by necessity, enormous. So why would criminals take the risk?

The simple answer is that they take the risk because ransomware has proven to be an enormously effective way of making a lot of money, very fast. There is also an aspect of “accuracy by volume” to ransomware, especially ransomware as a service.

Specialization allows each link in the ransomware-as-a-service supply chain to become significantly more efficient. They get more money for less effort this way. But there is also an aspect of simply overwhelming defenders with the sheer volume of attacks.

Cybercrime specialization mirrors specialization in other areas of endeavor. Just as there are teams engaged in technical documentation, marketing and even PR within legal organizations, criminal organizations also seek to employ the same talent.

Behind every ransomware attack there may be a supply chain consisting of thousands — even tens of thousands — of individuals. Today’s serious cybercriminals are emphatically not the proverbial lone malicious actors working out of their basements.

Does Cyber Insurance Make Ransomware More Lucrative?

Some people believe the mere existence of cyber insurance is making ransomware attacks more frequent and leading to bigger ransom demands.

Criminals engaging in BGH (reference earlier "big game hunting" definition) conduct reconnaissance before a ransomware attack. If possible, they determine whether an organization has cyber insurance and how much coverage they have, which can affect the size of the ransom demand.[1]

There's no industry-wide minimum standard for how well an organization must defend its network to be eligible for insurance coverage. And some insurers do not actually check on their clients' defenses,[2] though this is changing as insurers become more involved and rates rise.[3]

Taken together, these factors can create a situation where criminals know that victims can afford to pay big ransoms but still aren't required to put much effort into security. This is good for criminals, but terrible for insurance companies. And insurance companies are taking notice.

Insurance is not a substitute for adequate investment in information security.[4] Companies who sell cyber insurance have seen an increase in the number and size of claims they are paying due to increasing ransomware activity. As a result, some insurers have set limits on the total dollar amount they will pay per claim.[5] Others will only pay for a certain percentage of the losses incurred.[6]

[1] https://www.darkreading.com/edge-articles/the-double-edged-sword-of-cybersecurity-insurance

[2] https://www.washingtonpost.com/politics/2021/09/14/cyber-insurance-may-not-be-making-companies-more-secure/

[3] https://www.businessinsurance.com/article/20210304/NEWS06/912340248/Cyber-insurance-rates-to-increase-20-50-this-year-Aon

[4] https://www.crowdstrike.com/blog/why-cyber-insurance-is-not-a-substitute-for-cybersecurity/

[5] https://www.canadianunderwriter.ca/insurance/cyber-insurance-caught-in-perfect-storm-as-losses-surge-coalition-canada-1004212044/

[6] https://www.darkreading.com/edge-articles/how-are-cyber-insurance-companies-assessing-ransomware-risk-

This is especially true in life-critical contexts, such as healthcare. If people are harmed — or die — because of IT compromise, the event will quickly become sensationalized in the media, leading to increased scrutiny by both insurers and government agencies.

Consider the infamous ransomware attack on a hospital in Dusseldorf, Germany. Due to the attack an ambulance was redirected to another hospital, and a patient died. The media quickly reported[7] this as the first death directly attributable to ransomware, although it was later reported[8] that the patient would have died either way.

Especially concerning in this incident was that the attackers in this case were not specialized; they didn't even know they were attacking a hospital (they thought they were attacking a university). The police contacted the attackers, informed them of the details, and the attackers handed over the decryption keys.[9]

This incident not only underscores the non-monetary impacts of ransomware in the healthcare sector, it also demonstrates the intense scrutiny that healthcare organizations face when compromised. And, insurers are starting to notice.

The price of cyber insurance is rising. In 2021, insurance premiums were 7% to 40% higher than in 2020, depending on the size of the business being insured.[10]

Some ransomware-related losses may not be eligible for coverage. In May 2021, global insurer AXA announced that it would not reimburse companies based in France for ransom amounts paid to criminals.[11]

Other insurers are refusing to pay losses related to ransomware attacks by nation-state threat actors, insisting that these count as "acts of war,"

[7] https://arstechnica.com/information-technology/2020/09/patient-dies-after-ransomware-attack-reroutes-her-to-remote-hospital/

[8] https://www.schneier.com/blog/archives/2020/11/on-that-dusseldorf-hospital-ransomware-attack-and-the-resultant-death.html

[9] https://rp-online.de/nrw/staedte/duesseldorf/uniklinik-in-duesseldorf-ermittlungen-nach-tod-einer-frau-nach-hacker-angriff_aid-53407565

[10] https://www.darkreading.com/risk/ransomware-losses-drive-up-cyber-insurance-costs

[11] https://www.darkreading.com/risk/cyber-insurance-firms-start-tapping-out-as-ransomware-continues-to-rise

which are usually specifically excluded from insurance coverage.[12] Six members of the Russian military have been indicted by the United States for their role in the NotPetya attacks, which disrupted several major multinational corporations. Lawsuits about whether or not victims of these attacks qualify for insurance payouts are still ongoing.[13]

And although there may not be industry-wide requirements for minimum basic security precautions, individual insurers are starting to be a lot stricter about requiring that their customers practice good security hygiene to qualify for insurance.[14]

Given the huge financial risks associated with ransomware attacks, buying cyber insurance coverage seems like a no-brainer. However, getting coverage is not as easy or as cheap as it used to be. Expect to pay higher premiums for lower coverage — and expect insurers to take an interest in the quality of your defenses.

[12] https://www.cpomagazine.com/cyber-security/lloyds-of-london-cyber-insurance-will-not-cover-cyber-attacks-attributable-to-nation-states/amp/?

[13] https://www.darkreading.com/attacks-breaches/-act-of-war-clause-could-nix-cyber-insurance-payouts

[14] https://www.darkreading.com/edge-articles/the-double-edged-sword-of-cybersecurity-insurance

The Exploit Market

The buying and selling of software vulnerabilities, known as "exploits," is the most obvious place in the ransomware-as-a-service ecosystem where the criminal malware supply chain overlaps with the nation-state cyber warfare supply chain. Everyone buys exploits: governments, criminals, even software vendors.

The maturity of the exploit market has led to its specialization. Each exploit broker has a different clientele, but exploits can eventually be sold by multiple brokers into multiple different markets before the vendor finds out about it and has time to patch.

Some vendors have responded with bug bounty programs, effectively offering to buy the vulnerabilities before they hit the exploit broker market. But support for these programs is not universal among vendors. In many cases, exploit vendors can also pay more for an exploit, or can simply be easier to deal with than a vendor.

IT infrastructure is another popular target. Numerous vulnerabilities in corporate VPN servers came to light in 2020 and 2021.[29] Organizations that did not immediately patch became vulnerable, and many were compromised.

The exponential growth of ransomware over the past several years leaves no room for interpretation: The big game hunters of the exploit world have been working on the same targets for long enough to have learned their quarry. In addition to the everyday "spray and pray" attacks, high-profile organizations now have to contend with attackers who are starting to specialize in hacking them.

And in response, an ecosystem is emerging to help organizations of all sizes deal with the rise of ransomware as a service. Chief among these tools is threat intelligence.

[29] https://www.crowdstrike.com/blog/vulnerability-roundup-10-critical-cves-of-2020/

CHAPTER 4

The Ransom Dilemma

Let’s say the worst has happened: Despite your best efforts at defense, you’ve been hit by ransomware. You can’t access critical files. Entire departments are trying to get work done using pencil and paper. Some of your employees can’t do any of their work at all and are asking if they should just go home.

Providers may be facing loss of access to medical records, lab results and imaging. There may be problems booking appointments or making specialist referrals. IoT devices and patient monitoring equipment may be offline, and software supporting people responsible for real-time decision making, such as emergency triage or ambulance routing, may be unavailable.

There’s also the specter of really unfortunate data leaks, if it’s that kind of ransomware attack: pay up, or personally identifiable medical records and test results get released on the dark web. Those sorts of data breaches result in lawsuits.

In these situations tempers get short. There are complaints. Phones are ringing. Social media is full of anger and speculation. Journalists are asking awkward questions.

Your IT staff is still trying to figure out the full extent of what has been lost, and what, if anything, can be safely brought back online without spreading the infection further, all of which is complicated by the attackers having found and encrypted some of the backup servers, making that data unrecoverable without paying the ransom.

Someone from the finance department is on the phone with your insurance provider. The call has been going on for a worryingly long time; no one seems to have a straight answer about whether or not your coverage applies in this situation, and the press are interviewing burned-out staffers in the parking lot.

And absolutely everyone wants to know: Are you going to pay the ransom or not?

It's an unpleasant, chaotic, high-pressure situation. Ransomware operators know this and plan to take advantage of the pressure you're under.

Ransom demands often come with short deadlines attached and warnings of dire consequences if the deadlines are missed. Delay too long in responding or paying the ransom, and the ransom demand often goes up. Criminals pile on additional pressure, threatening to delete your files or leak your sensitive documents if you don't pay up quickly.

Plan for the Worst

The purpose of this guide isn't to tell you whether to pay or not to pay. That's a decision each organization will have to make on its own, taking into consideration its unique legal and financial circumstances and its responsibilities to customers or service users.

However, it is absolutely true that your decision making can only be improved by carefully considering the costs, regulatory requirements, insurance implications and other potential consequences of a ransomware situation *before* it happens to you.

Criminals rely on your making poor decisions under pressure, and healthcare staff throughout healthcare organizations are going to be continuously under unsustainable pressure for the foreseeable future. Consider your options and plan your possible responses ahead of time, so in a high-pressure scenario you can just reach for your established playbook.

Don’t Go It Alone

Dealing with the reality of ransomware as a service starts with threat intelligence. Threat intelligence exists to give organizations the ability to understand a threat actor’s motives, targets and attack behaviors.

Knowing your enemy is important, and different attackers may merit different responses. Depending on your information security team’s level of experience, they may handle certain commercial malware attackers themselves, while calling in professional digital forensics and incident response (DFIR) consultants for others.

A high-profile network breached by an attacker merits a law enforcement investigation, but a high-profile network breached by a confirmed nation-state actor may require a national security investigation. The sooner into an incident that the attacker can be identified, the fewer errors are likely to be made in responding to the event.

Developing an Incident Response Plan

Ask yourself these questions as you develop your incident response plan:

- **Know who needs to be informed in the event of a ransomware attack, and have a plan to contact them. Some groups to consider:**
  - Leaders in your organization
  - Legal counsel
  - Finance department
  - Public relations
  - Law enforcement
  - Insurance providers
  - Incident response specialists
  - IT vendors or service providers
  - Patients, families and extra-organizational caregivers

- **How much authority does your information security staff have to make decisions and take independent actions in an emergency?**
    - When can they act alone?
    - When should they involve organization leaders or other departments?
    - What scope do they have to impose change before running afoul of either regulatory considerations or vendor support constraints?
- **What actions will IT staff take to minimize the spread of infection and determine which systems are affected?**
- **What actions will IT staff take to preserve any forensic evidence of the attack?**
- **Who will be responsible for making a statement to members of the public or the media?**
    - How much are they allowed to disclose?
    - Does any statement need to be a joint statement with governments/LEAs?
- **What actions will you take if you suspect attackers may have stolen additional credentials during the attack?**
    - Think outside your own network: Do you need to check third-party services?
    - Can this compromise spread to suppliers or customers via IT integrations?
- **Once the infection is contained and the extent of the damage is known, which systems are most important to bring back first?**
    - Which systems are absolutely vital to day-to-day operations?
    - Do these systems depend on any others?

For more resources about developing an incident response plan, see the Cybersecurity and Infrastructure Security Agency Ransomware Guide.[1]

[1] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

CHAPTER 5

Defending Yourself Against Ransomware

Of course, it would be best if you never needed to use these plans — if you could successfully stop ransomware before it gets a foothold in your network. Obviously, this short guide cannot cover in any meaningful detail on how to defend your network. However, the basics of modern network defense — prevent, detect, respond and predict — are easy enough to learn so you can ask the right questions.

- **Prevent:** Harden systems through activities such as applying patches and reviewing permissions. Misdirect attackers using tools such as honeypots, and focus on the overall reduction of your attack surface.

- **Detect:** Identify signs that a compromise has occurred, and determine the extent of the compromise as quickly as possible. Contain the compromise and perform a risk assessment to decide how to proceed.

- **Respond:** Perform an investigation into the incident. Identify the vulnerabilities (technological as well as business process) that allowed the incident to occur. Remediate the vulnerability.

- **Predict:** Inventory your IT and OT assets. Know what you have and what it does. Baseline your most critical and most vulnerable systems and monitor them. If they do something unexpected, investigate. Look for vulnerabilities in your information security posture and remediate them before someone else finds them.

Defense in Depth

It takes a combination of technology, staff training and continuous business process improvement to keep an organization secure. Information security technologies need to be applied to individual devices (for example, next-generation antivirus), as well as at the network level (firewalls, threat feeds, CASB and so on).

No matter how hard you try, however, there is always a risk that disaster can strike. Even if you had a highly improbable set of network defenses capable of preventing 99.9999% of attacks, when attackers are throwing hundreds of thousands of attacks per year at you, compromise is inevitable.

This is why backups are a must: If your data doesn’t exist in at least three places, then it does not exist. But data backups aren’t enough — data is useless unless you can do something with it.

If the time it takes to restore all of your data is measured in months, then there is likely going to be a problem. This means that in addition to backups, a proper disaster recovery plan is a must. Also, keep in mind that modern ransomware tries to find and infect backups wherever possible; you need to store yours in a place that is not connected to the rest of your network.

Regular external audits can help you identify holes in your security posture. Data audits can also help you identify data that you can safely delete: You can’t have a data breach of data you don’t have!

Get Help

It’s important to remember that information security standards, certification, and regulatory compliance are only the beginning. Each network is different, and your security posture should be regularly reviewed by outside experts, but healthcare organizations should pay particular attention to network segmentation. The unique level of vulnerability in this sector makes isolating systems and devices to prevent lateral spread quite literally a life-critical consideration.

Defending any high-profile network is going to require bringing together expertise in hundreds of different technologies. It takes entire teams just to understand how those networks interconnect.

Cloud adoption doesn't remove the need to focus on information security. You still have to secure, back up and even plan for disaster recovery with cloud-based workloads and services. You need the expertise available to not only administer your cloud-based IT, but assess its security posture.

Managed security service providers (MSSPs) exist to help with some of this, but success is best achieved when they partner with internal teams. Both internal and external teams frequently find vulnerabilities the other doesn't.

Build your incident response connections before you need them. What do you do if your security measures fail? Do you know whom to call at which law enforcement agencies? Do you have the number of a professional negotiator who can help you deal with ransom demands? Do you have a crisis team ready to deal with the fallout of data leaks?

Gain Intelligence About the Threats

The sheer volume of attacks that ransomware as a service enables has made ransomware attacks on high-profile networks an inevitability. Planning for what to do when the worst happens is just as important as the effort that goes into preventing these incidents in the first place.

Different attackers call for different responses, and threat intelligence provides organizations the information necessary to make the right call at the beginning of an incident, when it matters most.

As you've learned throughout this Gorilla Guide, ransomware is growing in sophistication and ease-of-use. That's the bad news. The good news is that new tools are being developed daily to combat the threat, and partners are available to help you meet the menace of ransomware head on.

What is critical, though, is that you don't wait. Start preparing right now, because they're coming for you. Consider a solution from an experienced vendor like CrowdStrike that specializes in stopping the bad guys and getting you back on your feet if the worst does happen.

Take the next step in your cybersecurity journey and meet with our team. We can provide a complementary threat intelligence briefing for your organization or help assess your security maturity. Visit https://go.crowdstrike.com/ransomware-for-healthcare-ebook.html.

Resources

- **Malicious Domain Blocking and Reporting (MDBR)**
- **Nationwide Cybersecurity Review (NCSR)**
  - https://www.crowdstrike.com/cybersecurity-101/ransomware/how-to-prevent-ransomware/
  - https://www.cisecurity.org/ms-isac/services/mdbr/
  - https://www.cisecurity.org/ms-isac/services/ncsr/
  - https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident
  - https://csrc.nist.gov/projects/ransomware-protection-and-response
- **CISA Checkups and Trainings**
  - https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware
  - https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf
  - https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

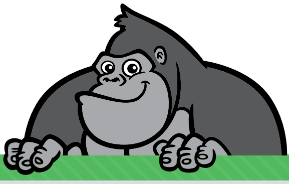
ABOUT ACTUALTECH MEDIA

ActualTech MEDIA

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.



If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit https://www.gorilla.guide/custom-solutions/