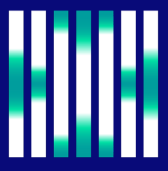
Held Hostage: Combatting the Growing Threat and Costs of Ransomware



UncommonX

Table of Contents

1 Introduction

In a digital-driven world where malware and other malicious threats cause chaos and damage to companies every day, one threat looms far above the rest: ransomware. It's one of the worst and most effective, which is why it has quickly become the preferred weapon for cyber criminals.

Ransomware is malware that shuts down businesses by blocking access to devices and entire systems. It literally holds organizations hostage until they pay a fee. Attackers (aka threat actors) can also use it to steal valuable and/or private data that they may release publicly or sell to the highest bidder if they don't receive payment.

The number of global ransomware attacks against businesses of every size rose 150% in 2020 and has already increased 151% in the first half of 2021.[1] In the United States alone, ransomware accounted for 30% of all cyberattacks reported to and confirmed by data breach researchers in 2020. That's more than double the rate for the entire world.[2] The FBI has warned that there are now 100 strains circulating the globe.[1]

The total cost of damages attributed to the attacks is expected to hit $20 billion by the end of 2021. That's 57 times more than the $325 million in 2015.[3] And it won't stop there. Industry experts expect damage costs to skyrocket to over $265 billion by 2031.[3]

And that's just based on attacks about which the authorities know. Most incidents go unreported, so it's impossible to tell exactly how many there were or how many companies paid although experts estimate it's at least half.[4] Also, no one knows for sure how many types of ransomware are still waiting to strike or are currently in development.

1 Introduction (cont.)

The objective of this white paper is to provide a deeper understanding of ransomware, including its history, types, and examples of recent attacks. It will also show the potential costs victims face, which are substantially more than just the ransom. Finally, it also provides basic suggested measures to help organizations increase security maturity so they can protect themselves against ransomware, as well as emergency steps to take immediately if they find themselves under attack.

2 History and Evolution of Ransomware

On November 2, 1988, a malicious program was released onto the internet from a computer at the Massachusetts Institute of Technology. Later dubbed the Morris Worm, it spread like wildfire. Within 24 hours, it infected one tenth of the approximately 60 thousand computers connected to the internet at the time, causing them to shut down.[5] Robert Tapan Morris, who created the worm, said he was "just trying to gauge how big the internet was."

Since then, hackers and other cyber criminals have been creating nastier ways of crippling digital devices and entire networks and for much more nefarious reasons: to cause chaos and/or extort victims. Today, there are an estimated one billion malware programs – that authorities know – with approximately 560 thousand new pieces detected every day.[6] That number is expected to continue increasing exponentially.

Of those programs, ransomware is now the go-to for criminals. This virulent and malicious software appeared a year after the Morris Worm. Known as AIDS or the PC Cyborg Trojan, it was sent to victims via floppy disc where it encrypted computers and the files on them. It forced users to either "renew their licenses" with the PC Cyborg Corporation by sending $189 or $378 to a post office box in Panama or risk never accessing their computers again.

2 History and lution of Ransomware (cont.)

Ransomware quickly became a much bigger threat. As internet technology and global connections expanded and improved, so did ransomware. It has become one of the fastest-growing malware hazards of the 21st century and a lucrative business model for criminals. Originally, it was used to hold individuals hostage. Now, it is aimed at much bigger targets like international corporations, universities, and even entire cities.

According to security think tank the Institute for Security and Technology, ransomware is no longer just a financial crime. It's an urgent national security risk that has affected the operations of critical resources, including military facilities.

3 How Ransomware Works and Why It's a Threat

Ransomware is malware that can cripple businesses, hospitals, schools, city governments, public infrastructure, and virtually any other type of organization. It works by infiltrating computers, networks, and/or mobile devices and then blocking user access. While there are countless strains, ransomware falls into two main types: crypto-ransomware, which locks specific computer files, and locker ransomware, which locks entire devices.

Attacks fall into two categories. The first is opportunistic ransomware campaigns. These are mostly automated and gain access to an organization's system through user-initiated actions like clicking on an unknown attachment in a phishing email or visiting a compromised website. Deploying these basic attacks require little technical know-how, which is why they are the most common.

But the second category is growing rapidly. That category is strategic ransomware campaigns. This is a more sophisticated process where threat actors go after specific larger targets or groups of targets. Victims are chosen based on criteria like their dependence on certain computer systems with known vulnerabilities, their level of network protection, and whether they can or will pay a ransom.

Once the malware infects a system, it swiftly and quietly seeps through every network-connected device, encrypting it or files using public key encryption. Users normally have no idea their system has been infected and compromised until it shuts down and a digital ransom "note" appears. Those notes can be as simple as a pop-up window or email to an executive or as dramatic as alerts flashing on every infected computer.

3 How Ransomware Works and Why It's a Threat (cont.)

The ransom is usually a demand for an online payment, most often in cryptocurrency, in return for the decryption key that will restore the user's locked files. A countdown clock may also appear, setting a deadline for the payment and threatening dire consequences if it isn't met.

To put even more pressure on victims to pay, hackers will steal valuable information during an attack and threaten to release it publicly or sell it on the dark web.[3] This is known as "double extortion." They go after sensitive private data like financial records, patient files, and intellectual property. That's why organizations like hospitals, banks, and city governments are favored targets. Criminals also prefer healthcare and law enforcement targets because they may be more willing to pay if a system shutdown means losing lives.

Ransomware has become such a successful form of attack that some developers are now offering it to others on the dark web as ransomware-as-a-service (RaaS). They "lease" it to other criminals with little or no technical knowledge who then launch their own assault campaigns. In return, those users pay a portion of their profits to the original developers. In the meantime, the back-end developers use the money earned by ransomware to continue to improve their "products" and devise more effective ways to bypass stagnant security measures, software defenses, and governmental requirements.

4 Examples of Major Ransomware Attacks

Nearly 2,400 healthcare facilities, schools, and governments in the United States were hit by ransomware in 2020 alone. That's according to the Ransomware Task Force, a group of more than 60 experts from industry, government, and universities that presented an 81-page report to President Joe Biden's administration.[7]

Major corporations have been targeted because they can pay the largest ransoms. But small- and mid-sized businesses (SMBs) are also under attack. In fact, research shows that there is little difference between the number of attacks on small organizations (those with less than 1,000 employees) and larger organizations (those with more than 1,000 employees).[8] Criminals know SMBs are usually ill-prepared for an assault, so they will more likely pay faster to regain access to their systems.

Although, based on news reports the past few years, several major corporations weren't ready to fend off ransomware assaults either. Attacks on those bigger entities also have a more widespread and detrimental effect on other companies, customers, and even the world at large.

Here are just a few recent examples of those cases.

WannaCry: In May 2017, a potent ransomware called WannaCry (aka WannaCrypt and Wcry) created havoc worldwide. Over 300 thousand people using Microsoft Windows in over 150 countries were hit during a two-day period. At the time, it was the largest ransomware attack ever. Businesses, governments, and individuals received digital ransom notes demanding $300 in Bitcoin to unlock encrypted files. It also threatened to double the price after three days and to

delete files if the ransom wasn't paid within a week.

Related costs (including the ransom, recovery expenses, legal fees, and more) were tallied at about $8 billion. Not only did it cause financial mayhem, but it also put lives at risk. Systems were shut down in healthcare companies across the United Kingdom. They were forced to cancel patient appointments, and hospitals were even telling people to avoid visiting emergency rooms. Microsoft later issued patches for its vulnerability, including for operating systems it no longer supported, which it had never done.[4]

NotPetya: In the fall of 2017, an incredibly vicious ransomware corrupted thousands of organizations in the U.S., Europe, Russia, and Australia. Not only did it encrypt files, but it also encrypted hard drives, preventing computers from loading their operating systems. Attackers asked for $300 in Bitcoin. But even when users paid it, the malware still caused irreparable damage, which indicated its goal wasn't to just rake in money but also to wipe data.

At first, authorities thought the ransomware may have been one called Petya. Others said it was something else, giving it the name "NotPetya." Researchers later discovered it was an even more dangerous combination of ransomwares GoldenEye, a variation of Petya, and WannaCry.[4]

Bad Rabbit: Around the same time NotPetya was unleashed, another ransomware called Bad Rabbit was disrupting thousands of computer systems across the U.S., Russia, and Ukraine. Authorities blamed the attack on the group Black Energy who they also believed was behind NotPetya.

Bad Rabbit started with the hacking of files on Russian media websites and the demand of 0.05 Bitcoin payment (about $275 U.S. dollars) with victims receiving 40 hours to pay before the ransom went up. The attack didn't last for a long time, indicating the controllers shut it down themselves.[4]

4 Examples of Major Ransomware Attacks (cont.)

Blackbaud: In 2020, hackers struck a South Carolina cloud software provider, stealing the data of thousands of users across the United States and Canada. Although Blackbaud paid the ransom, data breach laws required the firm to notify its clients, which included schools and hospitals, in dozens of states. The company was then hit with almost two-dozen class action lawsuits.[4]

Colonial Pipeline: This energy company accounts for 45% of the fuel supply for the U.S. East Coast, including homes, businesses, and even the military. In May 2021, it was forced to shut down operations and its 5,500-mile pipeline when a ransomware attack locked up several of its computers and demanded money to release them. Colonial Pipeline paid $4.4 million to obtain the software decryption key. But it took nearly a week to restore critical systems. That delay led to fuel shortages throughout the southeastern states.

DarkSide, a little-known group acting as a ransomware-as-a-service operation, was behind the attack. The incident showed that even a small group can still cause massive disruption. After facing the critical shortages at gas stations, the U.S. government refocused its attention on the importance of cybersecurity and encouraged companies and other organizations to do the same.[4]

JBS: The computer network of the world's largest meat processing company was attacked in June 2021. It shut down some of its vital operations in the U.S., Australia, and Canada. The sudden disruption in JBS's supply chain threatened to raise food prices for consumers. Hackers sent a ransom note saying they would also start deleting files if the company didn't pay $11 million in Bitcoin.

Even though a majority of JBS's plants weren't affected, executives paid the ransom anyway, saying it was necessary to protect customers. The attack was so sophisticated, they feared more of their operations would be compromised. The White House released a statement blaming the attack on a hacker group "likely based in Russia."[9]

4 Examples of Major Ransomware Attacks (cont.)

Kaseya: In July 2021, Kaseya, an information technology company with around 40,000 customers, announced it had suffered from a ransomware attack on its VSA software. This set of tools helps IT departments manage computers remotely. Kaseya reported that only 40 of its customers were affected. But they are all large IT companies serving hundreds of other businesses connected to thousands of users.

Over a thousand users were confirmed to have been affected, but that number is expected to grow. Investigators believe that with the large number of companies put at risk, it could end up being one of the largest ransomware attacks in history. A Russian hacker group called REvil was behind the assault. They didn't steal sensitive information, but they did send ransom notes demanding $50,000 from smaller companies and $5 million from larger ones.[10]

5 The Total Financial Impact of a Ransomware Attack

Ransomware cases increased 150 percent in 2020[11] and 151 percent in the first six months of the year.[1] The amount paid by victims jumped more than 300% in 2020.[11] DarkSide, the hacker ring behind the Colonial Pipeline attack, collected $14 million in ransoms in 2020 but extorted over $46 million in just the first three months of 2021.[4] With payouts like that, ransomware attacks are extremely profitable for criminals, so they won't be stopping any time soon.

For victims, paying ransoms ranging from hundreds of thousands to millions is bad enough. But that's just a sliver of the financial impact they may suffer. They also face associated costs, including, but not limited to, downtime, lost revenue and customers, missed sales opportunities, civil lawsuits, damage to their reputation, penalties for failed contract obligations, and governmental fines for noncompliance.

That's if companies pay the ransom. The amount may be much, much steeper if they don't. If they do pay some hackers may still not send the decryption key. They're criminals. It isn't like they're trustworthy. In either case, victims now must recover damaged or lost files and corrupted networks. That adds even more downtime – possibly weeks or months – and operational costs to the total tally.

Next, factor in the cost of recovery. If organizations can handle the cleanup in-house, they must pay for overtime labor and resources for incident response efforts. Many companies, especially SMBs, can't do it alone. So, they seek help from managed security services providers (MSSPs) to complete the long

expensive road to recuperating. Then they still need to invest in a stronger security infrastructure so they won't fall victim again.

In some cases, organizations may also be required to notify their customers, partners, and vendors that they've suffered from an attack. If they fail to do so within a specific time, they could face strict penalties for noncompliance. Once the news gets out, it could lead to negative publicity, a drop in stock prices, lost revenue, and even lawsuits. But, if an organization can determine that sensitive data hasn't been compromised, it may be able to avoid disclosing it to the world.

According to the Ponemon Institute's *Cost of a Data Breach Report* 2021, the overall cost of a data breach has increased to $4.24 million. That's up 10% from 2020 and still increasing. It's also the highest average cost in the report's 17-year history. The top five industries with the highest average total cost were healthcare ($9.23 million), financial ($5.72 million), pharmaceuticals ($5.04 million), technology ($4.88 million), and energy ($4.65 million).[12]

It's expected to get worse. A lot worse. The cost of ransomware incidents worldwide is estimated to exceed $265 billion by 2031. That's based on ransomware hitting both enterprises and consumers at a rate of one attack every few seconds. The dollar figure is based on 30 percent year-over-year growth in damage costs over the next 10 years.[3]

Cybersecurity insurance is available, but the consistent attacks are making it harder and more expensive to get coverage. Premium costs have risen almost 50 percent in 2021. Some carriers have been forced to stop offering it because when ransomware became the dominant criminal business model, insurance firms began losing millions in payouts.[5]

6 Protect Against Ransomware by Being Proactive

Ransomware attacks will only continue to grow in size and severity. Experts and law enforcement agree that the best way to safeguard against them is for organizations to be proactive. Stop attacks before they happen by strengthening security maturity levels. Opting to merely deploy basic security processes or simply comply with government requirements may not be enough though. Just being compliant doesn't always mean organizations are truly protected because federal and other regulatory requirements often lag far behind evolving threats.

There are ways to combat ransomware. But a truly effective program takes more than just installing the latest security tools. It's comprised of a combination of the right technology, in-depth processes, and knowledgeable people. It should also integrate security goals with a company's business objectives. That way organizations are protected without disrupting their ability to operate.

Here are some basic steps to help safeguard against ransomware and other cyber threats:

- Implement and update robust cybersecurity and business continuity strategies
- Locate system gaps and other weaknesses and fix them
- Ensure you have the right tools installed in the right places
- Install antivirus software on all your devices and update software regularly
- Back up data frequently and store multiple copies with at least one copy off-site

6 Protect Against Ransomware by Being Proactive (cont.)

- Provide regular security awareness training to your entire workforce
- Require strong passwords and multiple authentications for all accounts
- Scan all incoming and outgoing emails to detect potential threats
- Restrict which users can install software which may contain malware
- Block access to malicious IP addresses by configuring secure firewalls
- Develop strong business continuity plans and incident response plans

Finally, be vigilant. Cybersecurity isn't a one-and-done situation. Ransomware and other threats constantly evolve. Security needs to do the same on a continuous basis.

7 Steps to Contain and Combat a Ransomware Attack

While having a vigorous defensive program is strongly recommended, no preventive measures are guaranteed to stop ransomware or other malware 100% of the time. So, if an organization does find itself under attack, it's critical that IT and security teams respond as quickly as possible. It's also extremely important to have a comprehensive incident response (IR) team and plan in place as part of a mature security program.

The 2021 Ponemon Institute *Cost of a Data Breach Report* revealed that IR preparedness was the highest cost saver for businesses. The average total cost of a data breach for companies with an IR team that tests its plan regularly was $3.29 million compared to $5.29 million for companies without an IR team or those that didn't test their IR plan. That's a difference of $2 million.[12] That's a substantial savings for larger organizations but especially for SMBs with modest revenue and tight budgets.

If an attack occurs, the first step executives usually consider is whether to pay the ransom. That is a decision each organization must make for itself. But law enforcement and security experts have agreed that paying it is rarely the right option. Over half of the victims who do pay don't recover files. Either the hackers don't deliver the decryption key afterwards or they do but the keys don't work. The FBI also advices against paying because that money helps fund the development of more dangerous malware.

Below are steps to take in case of an attack. Following these actions as quickly as possible can help avert the severe loss of data, time, and money.

7 Steps to Contain and Combat a Ransomware Attack (cont.)

- Disconnect all infected devices from the network immediately to prevent the ransomware from spreading
- Notify the IT team right away so they can implement incident response and other procedures
- Inform employees that there has been a breach and to follow established protocols
- Change all administrative and user login credentials
- Restore data backups after the threat has been removed and security updates are completed
- Identify the type of ransomware and collect other evidence to prevent future incidents
- Take a photo of the ransom note with a mobile phone as evidence for the authorities and insurance claims
- Contact law enforcement to report the attack so they can investigate
- Update your security systems after the incident

If you feel your IT or security team doesn't have the resources to effectively manage incident response, then consider working with a Managed Security Services Provider (MSSP).

8 The Benefits of a Managed Security Services Provider

For many organizations, it's too cost-prohibitive to maintain a fully staffed, in-house IT security team capable of monitoring its network 24/7 and reacting to a ransomware attack. That's why many of them contract with a MSSP for help.

Here are the main reasons why it may be an effective and cost-effective solution:

Lower Cost – An MSSP is a portion of the cost associated with maintaining a 24/7, in-house program, including staffing, training, maintenance, and infrastructure.

Rapid Deployment and Immediate Benefits – System deployment by an MSSP is faster because it doesn't require remodeling of an organization's network infrastructure, customer technical expertise, or server management. Plus, MSSP professionals begin monitoring data and threats right away.

Integration of Multiple Technologies – An MSSP can integrate various data sources regardless of its type or manufacturer. This means little to no cost to replace existing IT assets, minimal setup costs, and a significant flexibility in how technology is applied.

Workflow and Event Response Prioritization – An MSSP can prioritize and coordinate responses to issues generated by threat events by utilizing a coordinated event management workflow that traditional in-house event logging/monitoring systems lack.

Scalability of 24/7 Security Resources – Programs can be tailored for any size

organization, no matter what its operating model and level of sophistication. An MSSP can also provide either full-time security or after-hours service to augment an existing in-house program.

Effective Handling of Security Incidents – MSSPs possess the skills and experience to triage and remediate threats in an effective and timely manner.

Detailed Analysis and Reporting – This information provides real-time information and comprehensive reporting so senior leadership can make more effective business decisions.

9 Conclusion

In the short time it took to read this paper, the number of ransomware threats and attacks continued to grow. And as they increase, so does the likelihood that it will strike your organization. Ransomware has become a significant global threat with the ability to totally cripple any organization – some beyond recovery. Ignoring the risk won't change that. Waiting for it to strike and then reacting is also not a recommended action due to potential damage and substantially increased costs.

Authorities and experts agree that the most effective way to protect against ransomware and other cyber threats is to be ready for them. Start now. Proactively defend your organization by first assessing your ability to proactively defend your organization. Then make the necessary changes to raise your security maturity level to where it needs to be – or even higher – to suit your objectives.

After that, regularly review and improve it. Ransomware and other threats constantly evolve. So should security programs. That alone can save organizations millions of dollars as well as lost data, time, and revenue.

10 Endnotes

1. Seals, T., "Ransomware Volumes Hit Record Highs as 2021 Wears On," *Threat Post*, August 3, 2021, https://threatpost.com/ransomware-volumes-record-highs-2021/168327

2. De Vynck, G., Lerman, R., Nakashima, E., & Alcantara, C., "The anatomy of a ransomware attack," *The Washington Post*, July 9, 2021, https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works

3. David Braue, "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031," *Cybercrime Magazine*, June 3, 2021, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031

4. Nakashima, E., & Lerman, R., "Ransomware is a national security threat and a big business – and it's wreaking havoc," *The Washington Post*, May 15, 2021, https://www.washingtonpost.com/technology/2021/05/15/ransomware-colonial-darkside-cyber-security

5. The Morris Worm: 30 Years Since First Major Attack on the Internet," The FBI: Federal Bureau of Investigation, US Department of Justice, November 2, 2018, https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

6. Jovanović, B., "A Not-So-Common Cold: Malware Statistics in 2021," Data Prot, March 20, 2021, https://dataprot.net/statistics/malware-statistics

7. "Combatting Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," Prepared by The Institute for Security and Technology, September 2021, https://securityandtechnology.org/ransomwaretaskforce/report

10 Endnotes (cont.)

8. Rudow, C., "The cost of ransomware attacks," Nationwide Insurance blog, August 1, 2020, https://www.nationwide.com/cps/cic/blog/cost-of-ransomware-attacks.html
9. "Meat giant JBS pays $11m in ransom to resolve cyber-attack," The BBC, June 10, 2021, https://www.bbc.com/news/business-57423008
10. De Vynck, G., & Lerman, R., "Widespread ransomware attack likely hit 'thousands' of companies on eve of long weekend," *The Washington Post*, July 3, 2021, https://www.washingtonpost.com/technology/2021/07/02/kaseya-ransomware-attack
11. Sharton, B., "Ransomware Attacks Are Spiking. Is Your Company Prepared?," *Harvard Business Review*, May 20, 2021, https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared
12. Paganini, P., "Cost of a Data Breach study: Cost of a Data Breach hits record high during pandemic," *Cyber Defense Magazine*, July 29, 2021, https://www.cyberdefensemagazine.com/ibm-cost-of-a-data

11 Contributors

Patrick Hayes, Chief Security Officer

Mr. Hayes is a seasoned business leader and certified Enterprise Security Architect with over 25 years of experience in information security strategy. During the course of his career, he has operated in several key senior roles accountable for strategic direction, architecture, and execution.

Devin Jones, Chief Product Officer

Mr. Jones is an accomplished executive leader with advanced experience building company infrastructures that define, design, build, and deliver product value and revenue growth. He has excelled at helping companies like Cisco and Juniper Networks establish new markets and identify growth.

Rick Holod, Vice President of Security Services

Mr. Holod is an accomplished IT risk/security leader with practical experience in several major industries. He joined the company in July 2021 with 30 years of in-depth knowledge in enterprise architecture, security risk management, conceptual and logical modeling, and business strategies.

About UncommonX

UncommonX offers unmatched enterprise-class cybersecurity protection for mid-size organizations by combining adaptive threat and intelligence software with 24/7 industry experts, making it easy to constantly both map and fix root causes of security vulnerabilities. Taking a market-first, inside-out approach to ongoing digital security risks through unique curated threat feeds and automated analytics, the UncommonX BOSS intelligent security platform provides clear contextual awareness to yield accelerated outcomes to mitigate and guard against threats.

UncommonX.com

640 N. LaSalle Drive, Suite 592, Chicago, IL 60654 USA

UNCOMMONX