Backblaze

The Complete Guide to Ransomware

Contents

Overview

Ransomware attacks are one of the biggest threats to businesses today, and the risk continues to rise. In 2023, the FBI's Internet Crime Complaint Center received 2,825 ransomware complaints, representing losses of more than $59.6 million,[1] and those are just the ones that got reported. Cybersecurity Ventures expects that by 2031, businesses will fall victim to a ransomware attack every other second,[2] up from every 11 seconds in 2021, every 14 seconds in 2019, and every 40 seconds in 2016—a sharp acceleration greatly influenced by the rise of remote work following the global pandemic.

And the largest ransom ever demanded hit $100 million in April 2024.[3] As ransomware becomes more sophisticated and cybercriminals demand bigger payouts, businesses and organizations big and small are well served to view protection as essential.

In this ebook, we review the current state of ransomware and the ransomware economy. We then walk through how ransomware attacks unfold and what you can do to protect your business or organization. We developed this ebook because, while the $100 million demands make headlines, unreported attacks devastate small and medium-sized businesses and organizations every day. Understanding how the ransomware economy works helps you understand the extent of the threat and the importance of preparing for a possible attack on your business.

What is ransomware?

Ransomware is a form of malware (malicious software) that encrypts a victim's files so they cannot be accessed. The attacker then demands that the victim pay a ransom in order to have their unencumbered access restored. Newer attacks include the exfiltration of a target's data before encryption, adding the public release of that data as a second layer of extortion to the attack.

1 https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
2 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
3 https://www.infosecurity-magazine.com/news/ransomware-demands-staggering-5m

Ransomware by the numbers

$100 million

Largest ransom demand to date.

75%

Percentage of attacks that target small to medium-sized businesses.

$1.1 billion

How much ransomware syndicates made in 2023.

$42 billion

Predicted ransomware damages for 2024.

23 days

Average downtime.

$1.54 million

Average ransom payment in 2023.

$1.82 million

The average bill for recovering from a ransomware attack, including downtime, people hours, device costs, network costs, and lost opportunities.

Current State of Ransomware

Ransomware has come a long way since the days when bad actors handed out infected floppy disks to unsuspecting victims. In terms of sophistication, cost, and increasing threats to organizations, ransomware is pervasive and on the rise. In this section, we'll cover ransomware's early evolution and how it affects different industries. We'll also highlight some notable attacks.

Growth and prevalence

The first ransomware attacks occurred in 1989 with floppy disks distributed across organizations, purporting to raise money to fund AIDS research. At the time, the users were asked to pay $189 to get their files back.[4] Since then, ransomware has taken advantage of multiple developments in technology, similar to other high-growth industries.

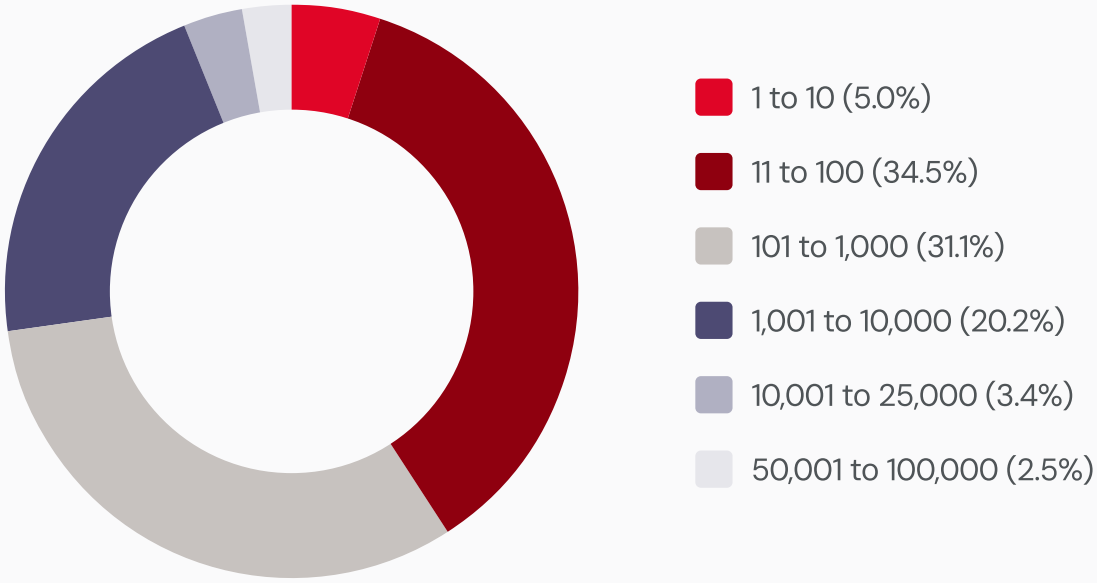
With the advent of multiple facilitators, ransomware has grown significantly since the mid-2000s. Sophisticated RSA encryption with increasing key sizes makes encrypted files more difficult to decrypt. Ransomware kits are now relatively easy to access on the dark web and only cost $70.[5] With cryptocurrency now firmly in place as a financial pathway, payment is both virtually untraceable and nearly irreversible. Sadly, as recovery becomes more difficult, the cost to victims rises alongside it. The frequency of attacks has increased as ransomware has evolved to be more accessible, more virulent, and stealthier at evading detection.

Industry trends and notable attacks

With total costs in the billions and threat actors demanding astronomical ransoms, small and medium-sized businesses (SMBs) and public sector organizations risk being lulled into a false sense of security by thinking cybercriminals set their sights on much larger enterprises. That false sense of security actually makes these entities prime, unsuspecting targets for ransomware attacks.

4 https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
5 https://www.techrepublic.com/article/how-much-malware-tools-sell-for-on-the-dark-web/

Ransomware Impacted Companies by Size (Employee Count)



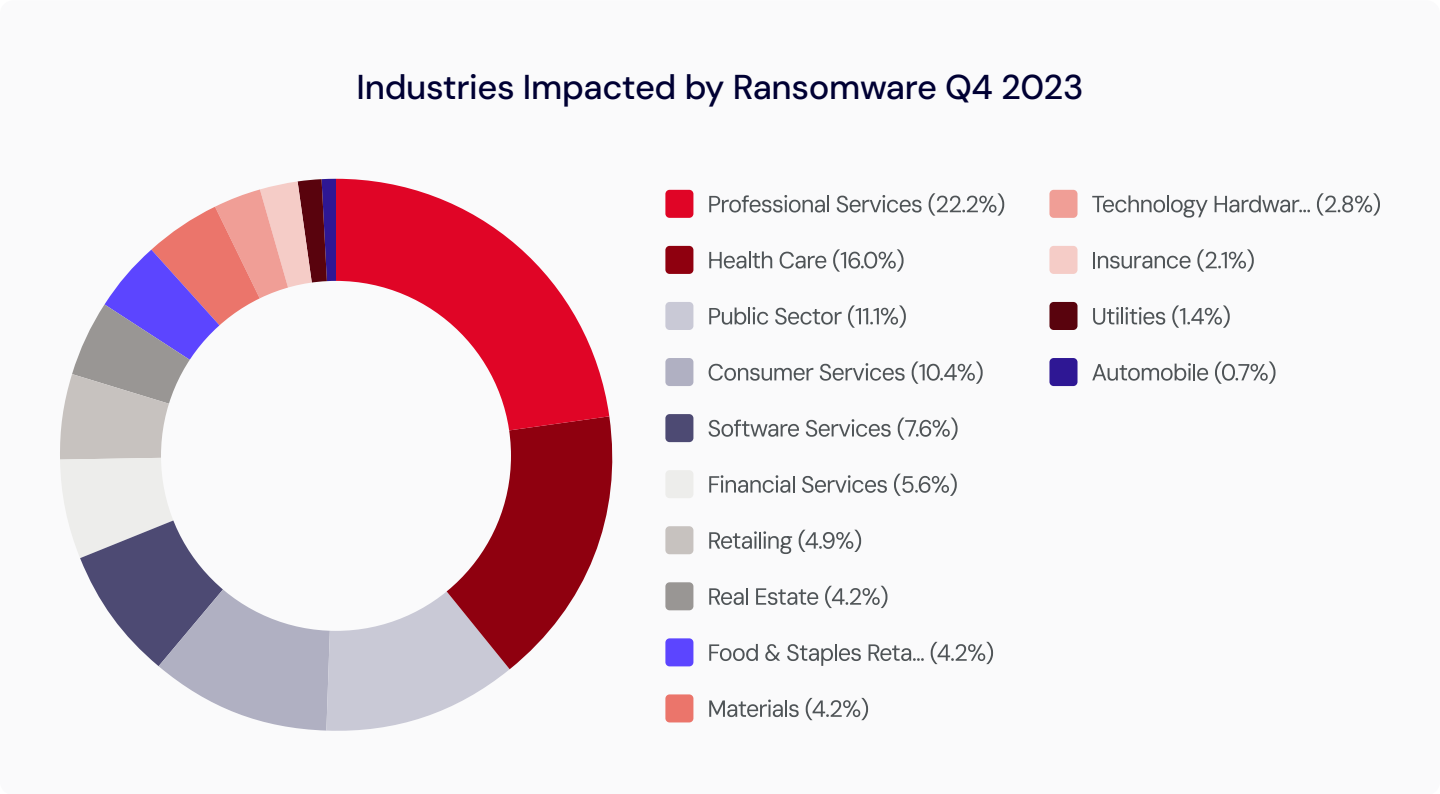
Source: Coveware Quarterly Ransomware Report.

> With total costs in the billions and threat actors demanding astronomical ransoms, small and medium-sized businesses (SMBs) and public sector organizations risk being lulled into a false sense of security by thinking cybercriminals set their sights on much larger enterprises. That false sense of security actually makes these entities prime, unsuspecting targets for ransomware attacks.

Why attackers target SMBs and the public sector:

- Constrained IT budgets.
- Lack of protections in place.
- More likely to pay a moderate ransom rather than risk downtime.

Based on 2023 data from the Small Business Administration, small businesses (defined as having fewer than 500 employees) accounted for 99.9% of all businesses.[6] Just as these businesses span every industry, so do ransomware attacks. From health care to insurance to higher education, these businesses have one thing in common: they all require sensitive user data to function, and sensitive user data is a cybercriminal's favorite target.s In 2021, 77 state and municipal governments and agencies were impacted by ransomware, making it the second-most-targeted sector behind academia.[7]



Source: Coveware Quarterly Ransomware Report.

6 https://advocacy.sba.gov/wp-content/uploads/2023/03/Frequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf
7 https://www.ic3.gov/Media/News/2022/220330.pdf

Here are just a few specific attacks from 2023.

Dish Network: In February 2023, Dish Network experienced a ransomware attack that caused widespread outages across its platforms, affecting websites, communications, and apps. The company initially described the issue as an "internal system issue" but later confirmed it was a cybersecurity breach. The attack compromised data of 296,851 individuals, including names and license numbers. It is reported that Dish likely paid the ransom demands.[8]

Prospect Medical Holdings: This attack occurred in August 2023 and affected California-based Prospect Medical Holdings, which operates 16 hospitals. The ransomware attack, claimed by the Rhysida gang, disrupted both inpatient and outpatient operations. The attackers accessed sensitive information, including health records and Social Security numbers, and put the data up for sale on the dark web. The attack caused significant operational disruptions, with systems only being fully restored by September 12, 2023.[9]

NCR Corporation: In April 2023, NCR, a financial services firm, was targeted by the BlackCat/AlphV ransomware group. The attack disrupted NCR's payment processing systems, particularly affecting the Aloha point-of-sale system and Back Office app. Although the company stated that only one data center was impacted and no customer financial information was stored there, the attackers claimed to have login credentials that could access client systems.[10]

> "To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity.
>
> – President Joe Biden[11]

The direct cost of recovering from a ransomware attack is often just the floor rather than the ceiling. In reality, the total cost of the attack is difficult to quantify as it comes not just from the ransom sums and longer downtimes, but also negative press, public mistrust, and time and money spent restoring data.

8 https://www.techtarget.com/searchsecurity/news/366564303/10-of-the-biggest-ransomware-attacks-in-2023
9 https://www.techtarget.com/searchsecurity/news/366564303/10-of-the-biggest-ransomware-attacks-in-2023
10 https://www.sangfor.com/blog/cybersecurity/list-of-top-ransomware-attacks-in-2023
11 https://www.nasdaq.com/articles/ransomware-is-the-greatest-business-threat-in-2022

The Ransomware Economy

Ransomware continues to proliferate for a simple reason—it's profitable. And it's profitable not just for the ransomware developers themselves—they're just one part of the equation—but for a whole ecosystem of players who make up the ransomware economy. To understand the threats to SMBs and organizations today, it's important to understand the scope and scale of what you're up against.

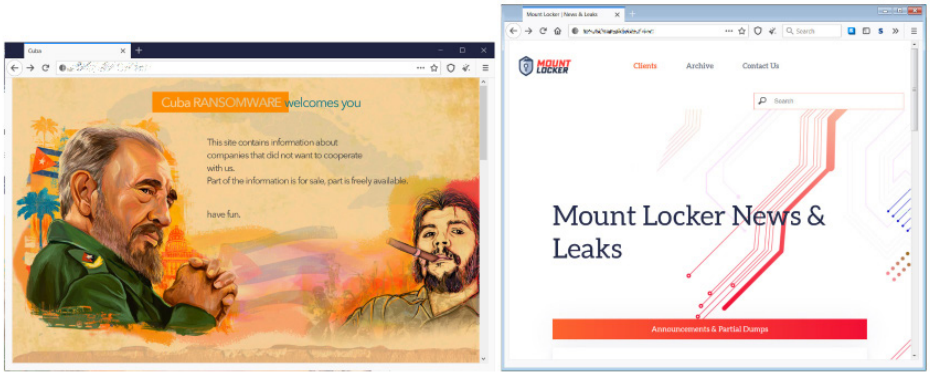
In this section, we'll identify the prominent ransomware syndicates working today and break down how they operate, including the recent emergence of ransomware as a service. Then, we'll illustrate the size of the ransomware economy based on how much ransomware operators make as well as the true, overall cost of ransomware attacks.

Top ransomware syndicates

Having an awareness of where attacks come from can prepare you if you ever face one yourself—your first task will be to identify the group you're fighting. Here, we'll start to illustrate the broader ransomware economy by describing the top ransomware syndicates in operation today.

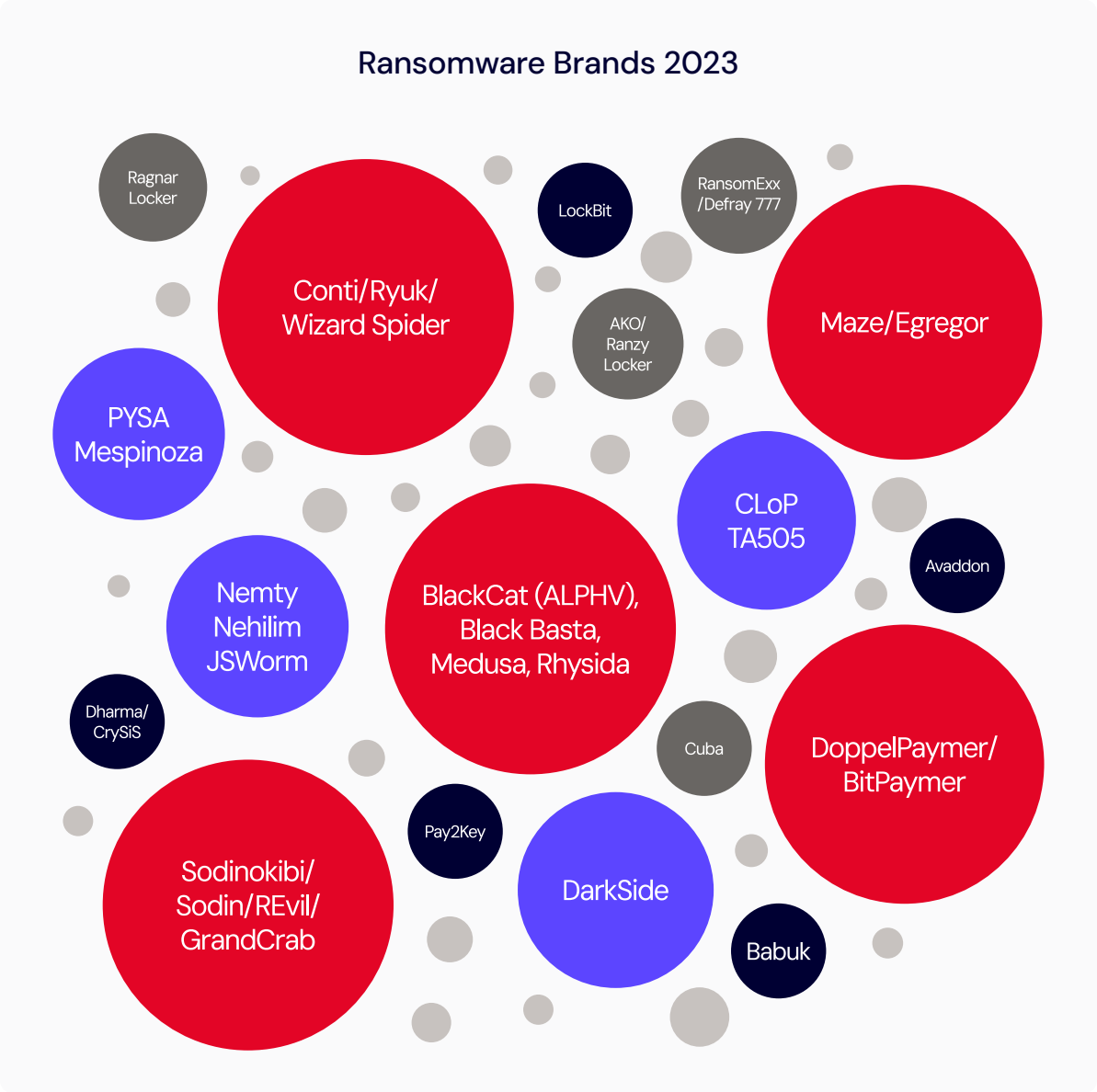
Cybercriminals have long been described as operating in "gangs." The label conjures images of hackers furiously tapping away at glowing workstations in a shadowy warehouse. But the work of the ransomware economy today is more likely to take place in a boardroom than a back alley. Cybercriminals have graduated from gangs to highly complex organized crime syndicates that operate ransomware brands as part of a sophisticated business model.

Operators of these syndicates are just as likely to be worrying about user experience and customer service as they are with building malicious code. A look at the branding on display on some syndicates' leak sites makes the case plain that these groups are more than a collective of expert coders—they're savvy business people.



Source: Bleepingcomputer.com.

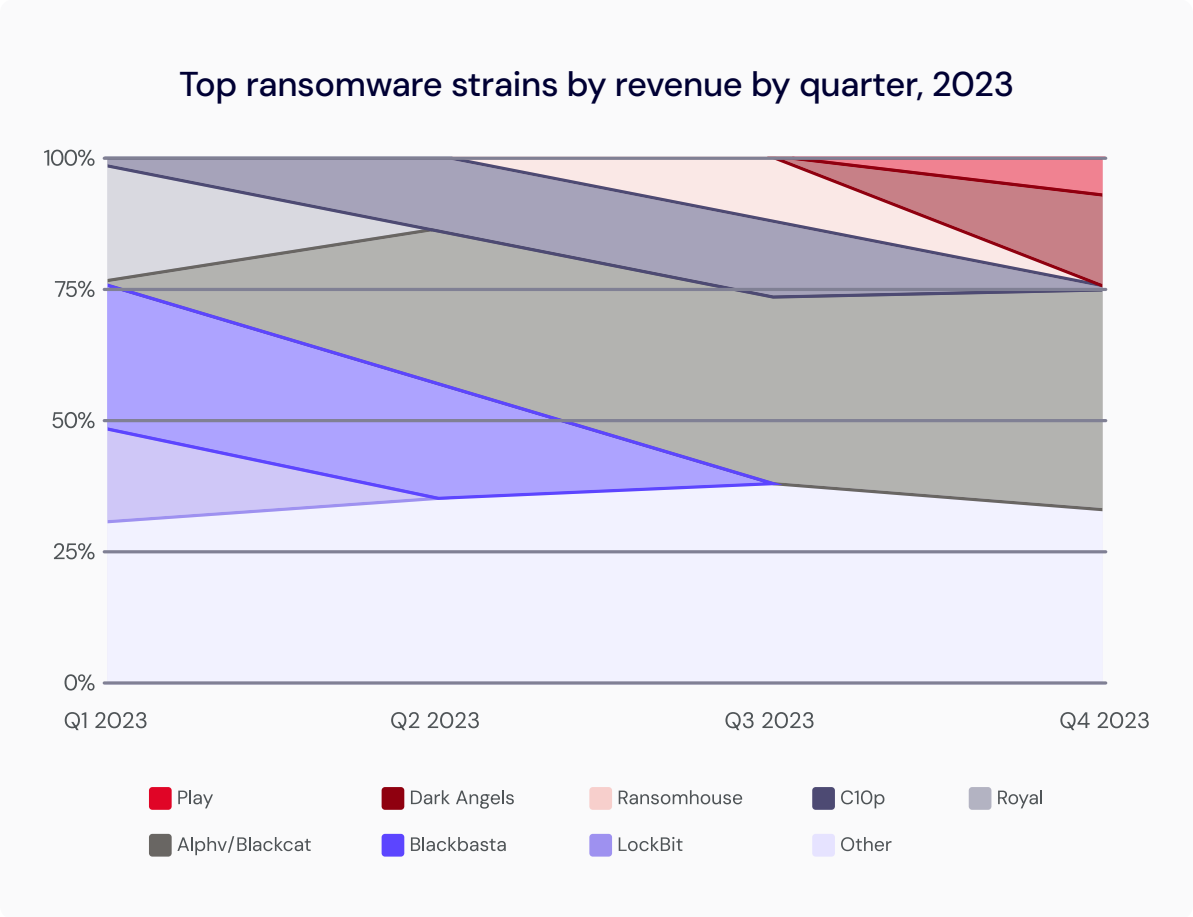
Ransomware operators are often synonymous with the software variant they brand, deploy, and sell. Many have rebranded over the years or splintered into affiliated organizations. Some of the top ransomware brands operating today along with high profile attacks they have carried out are shown in the infographic below.[12]



The groups shown above do not constitute an exhaustive list. In June 2021, FBI Director Christopher Wray stated that the FBI was investigating 100 different ransomware variants[13] and new ones pop up every day. While some brands have existed for years (Ryuk, for example), the list is also likely obsolete as soon as it's published. Ransomware brands bubble up, go bust, and reorganize, changing with the cybersecurity tides.

13 https://www.reuters.com/technology/fbi-says-it-is-investigating-about-100-types-ransomware-wsj-2021-06-04/

Research by Chainalysis shows just how much brands fluctuate year to year and, they note, even month to month:



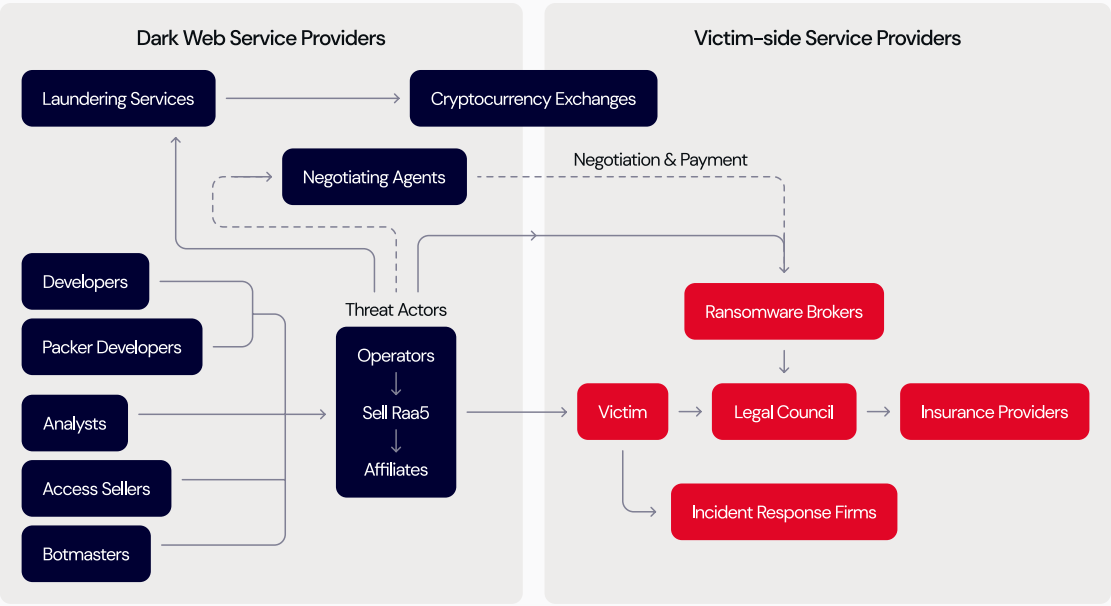
Source: Chainalysis.[14]

14 https://www.chainalysis.com/blog/ransomware-2024/

How ransomware syndicates operate

Ransomware operators may appear to be single entities, but there is a complex ecosystem of suppliers and ancillary providers behind them that exchange services with each other on the dark web. Now that you have an understanding of the major ransomware operators, this section arms you with information about the breadth of the ransomware economy by describing all of the players and how they interact, as illustrated in the flowchart below.

The Ransomware Economy



Developers

Write the ransomware software and sell it to the threat actors for a cut of the ransom.

Analysts

Evaluate the victim's Financial health to advise on ransom accounts that they're most likely to pay.

Access Sellers

Take advantage of publicly disclosed vulnerabilities to infect servers before the vulnerabilities are remedied, then advertise and sell that access to threat actors.

Botmasters

Create networks of infected computers and sell access to those compromised devices to threat actors.

Negotiating Agents

Handle interactions with victims.

Laundering Services

Exchange on cryptocurrency for fiat currency on exchanges or otherwise transform ransom payments into usable assets.

Operators

The entity that actually carries out the attack with access purchased from developers or developed in-house.

May employ a full staff, including customer service, IT support, marketing, etc. depending on how sophisticated the syndicate is.

Affiliates

Purchase ransomware as a service from operators anddevelopers who get out of the ransom.

Ransomware Brokers

Brought in to negotiate and handle payment on behalf of the victim and act as intermediaries between the victim and operators.

Legal Council

Often manages the relationship between the broker, insurance provider, and victim, and advise on ransom payment discision-making.

Incident Response Firms

Consultant who assists victims in response and recovery.

Insurance Providers

Cover victim's damages in the event of an attack.

Dark web service providers

Cybercrime "gangs" could once be tracked down and caught like the David Levi Phishing Gang that was investigated and prosecuted in 2005.[15] Today's decentralized ecosystem, however, makes going after ransomware operators all the more difficult. These independent entities may never interact with each other outside of the dark web where they exchange services for cryptocurrency:

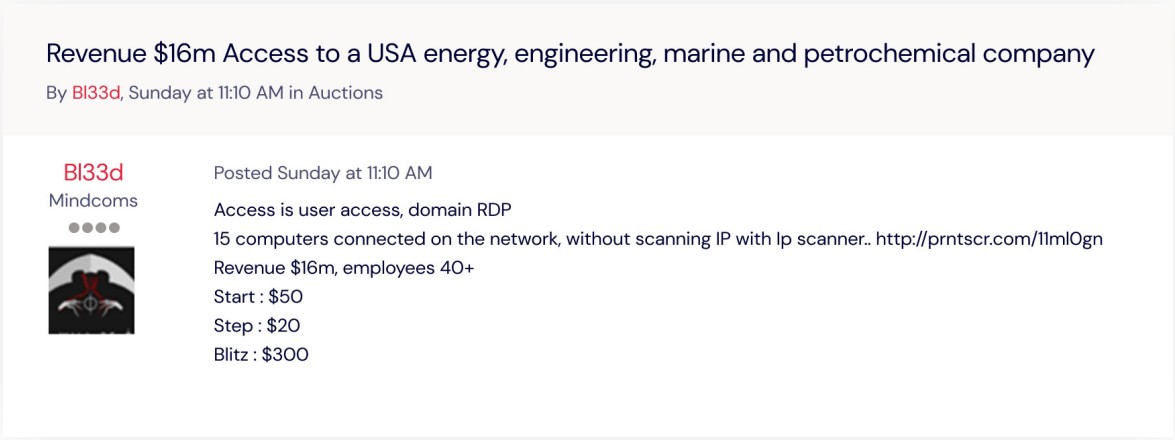
- Botmasters: Create networks of infected computers and sell access to those compromised devices to threat actors.
- Access sellers: Take advantage of publicly disclosed vulnerabilities to infect servers before the vulnerabilities are remedied, then advertise and sell that access to threat actors.
- Operators: The entity that actually carries out the attack with access purchased from botmasters or access sellers and software purchased from developers or developed in-house. May employ a full staff, including customer service, IT support, marketing, etc. depending on how sophisticated the syndicate is.
- Developers: Write the ransomware software and sell it to threat actors for a cut of the ransom.
- Packer developers: Add protection layers to the software, making it harder to detect.
- Analysts: Evaluate the victim's financial health to advise on ransom amounts that they're most likely to pay.
- Affiliates: Purchase ransomware as a service from operators/developers who get a cut of the ransom.
- Negotiating agents: Handle interactions with victims.
- Laundering services: Exchange cryptocurrency for fiat currency on exchanges or otherwise transform ransom payments into usable assets.

15 https://www.nbcnews.com/id/wbna9884895

Victim-side service providers

Beyond the collection of entities directly involved in the deployment of ransomware, the broader ecosystem includes other players on the victim's side, who, for better or worse, stand to profit off of ransomware attacks. These include:[16]

- Incident response firms: Consultants who assist victims in response and recovery.
- Ransomware brokers: Brought in to negotiate and handle payment on behalf of the victim and act as intermediaries between the victim and operators.
- Insurance providers: Cover victim's damages in the event of an attack.
- Legal counsel: Often manage the relationship between the broker, insurance provider, and victim, and advise on ransom payment decision-making.



Advertisement for access to an organization's RDP. Source: Threatpost.[17]

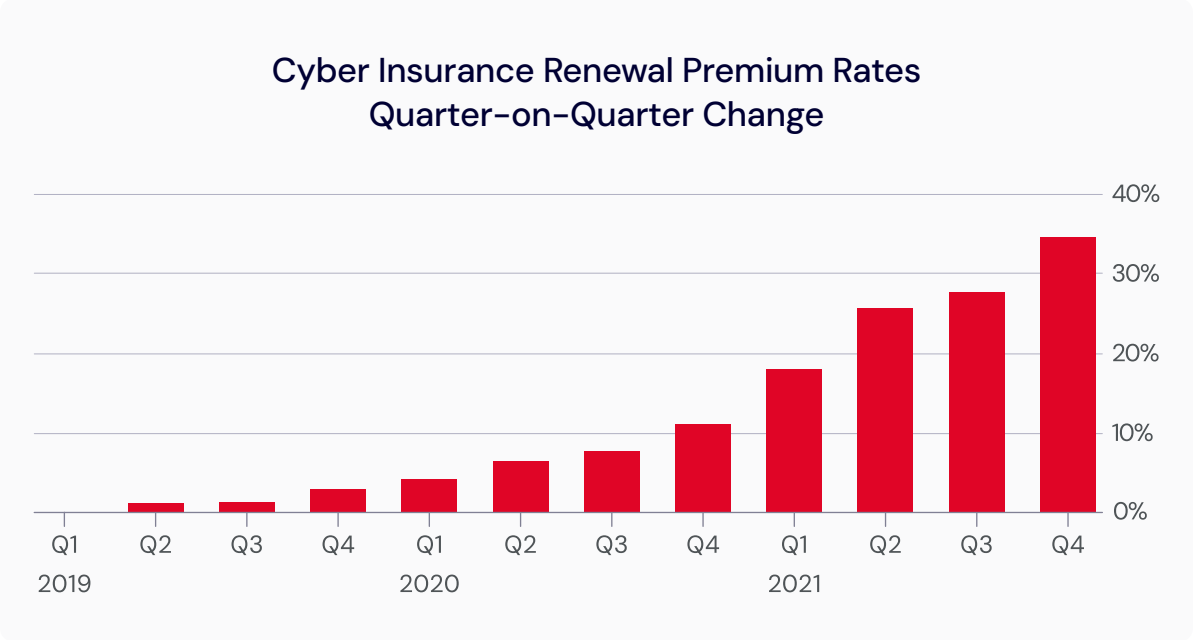
16 https://www.securityweek.com/inside-ransomware-economy
17 https://threatpost.com/ransomware-4k-cyber-underground/166145/

Are victim-side providers complicit?

While these providers work on behalf of victims, they also perpetuate the cycle of ransomware. For example, insurance providers that cover businesses in the event of a ransomware attack often advise their customers to pay the ransom if they think it will minimize downtime, as the cost of extended downtime can far exceed the cost of a ransom payment. This becomes problematic for a few reasons. First and foremost, paying the ransom incentivizes cybercriminals to continue plying their trade. And second, as Colonial Pipeline discovered, the decryption tools provided by cybercriminals in exchange for ransom payments aren't to be trusted. More than a month after Colonial paid the $4.4 million ransom and received a decryption tool from the cybercriminals, CEO Joseph Blount testified before Congress that recovery from the attack was still not complete. After all that, they had to rely on recovering from their backups anyway.

Cyber insurance is nothing new. For over a decade, providers have offered policies that cover outages from viruses, data lost to cybercrime, and other assorted online pitfalls. Ransomware claims, however, have skyrocketed—now accounting for nearly 75% of all claims filed.

Consequently, the cost of coverage has gone up, with premiums rising to unprecedented levels. Utility companies, already under the spotlight after Colonial, have seen increases of 25-30% in their premiums. In some cases, premiums have risen 74%.



Source: Fitch Ratings, Council of Insurance Agents & Brokers

Ransomware as a service

In the ransomware economy, operators and their affiliates are the threat actors that carry out attacks. This affiliate model where operators sell ransomware as a service (RaaS) represents one of the biggest threats to SMBs and organizations today.[18] This section describes the emergence of RaaS, how RaaS evolved in the ransomware economy, and the threat it poses to SMBs.

Cybercrime syndicates realized they could essentially license and sell their tech to affiliates who then carry out their own misdeeds empowered by another criminal's software. The syndicates, affiliates, and other entities each take a portion of the ransom.

Operators advertise these partner programs on the dark web and thoroughly vet affiliates before bringing them on to filter out law enforcement posing as low-level criminals. One advertisement by the REvil syndicate noted, "No doubt, in the FBI and other special services, there are people who speak Russian perfectly, but their level is certainly not the one native speakers have. Check these people by asking them questions about the history of Ukraine, Belarus, Kazakhstan or Russia, which cannot be googled. Authentic proverbs, expressions, etc."[19]

Though less sophisticated than some of the more notorious viruses, these "as a service" variants enable even amateur cybercriminals to carry out attacks. And they're likely to carry out those attacks on the easiest prey—small businesses who don't have the resources to implement adequate protections or weather extended downtime.

Hoping to increase their chances of being paid, low-level threat actors using RaaS typically demanded smaller ransoms, under $100,000, but that trend is changing. Coveware reported in August 2020 that affiliates are getting bolder in their demands. They reported the first six-figure payments to the Dharma ransomware group, an affiliate syndicate, in Q2 2020.[20]

The one advantage savvy business owners have when it comes to RaaS: attacks are high volume (carried out against many thousands of targets) but low quality, and easily identifiable by the time they are widely distributed.[21] By staying on top of antivirus protections and detection, business owners can increase their chances of catching the attacks before it's too late.

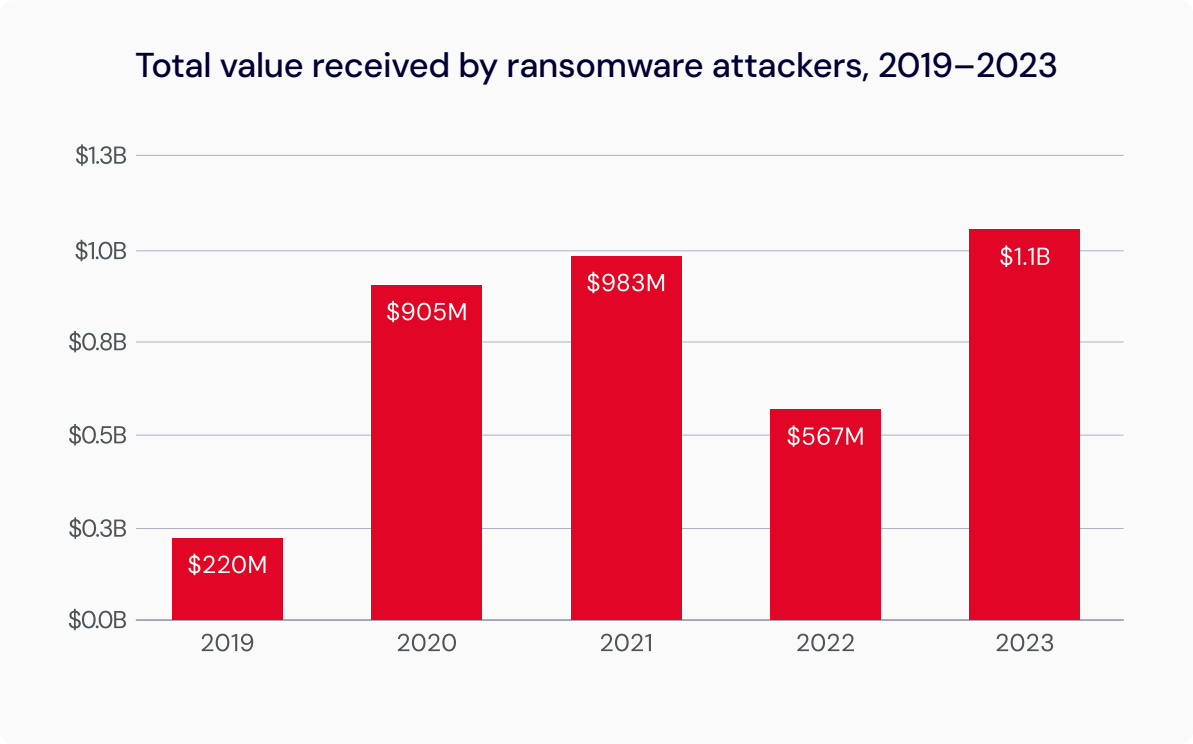
18 https://www.zdnet.com/article/ransomware-huge-rise-in-attacks-this-year-as-cyber-criminals-hunt-bigger-pay-days/
19 https://threatpost.com/inside-ransomware-economy/166471/
20 https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report
21 https://www.forbes.com/sites/forbestechcouncil/2020/11/10/the-evolution-of-the-ransomware-economy/?sh=3d1fdb5e7484

Ransomware revenue and profitability

Ransomware operators have a cache of weapons at their disposal to generate revenue. This section illustrates the size of the ransomware economy in financial terms and how ransomware operators turn ransom payments into usable cash.

How much money do ransomware crime syndicates actually make? The short answer is that it's difficult to know because so many ransomware attacks go unreported. To get some idea of the size of the ransomware economy, analysts have to do some sleuthing.

Chainalysis, a blockchain data platform, tracks transactions to blockchain addresses linked to ransomware attacks in order to capture the size of ransomware revenues. In their regular reporting on the cybercrime cryptocurrency landscape, they showed that the total amount paid by ransomware victims was over was over $1.1 billion in 2023, up from $567 million in 2022 and $983 million in 2021. They expect the number will only continue to grow.[22]



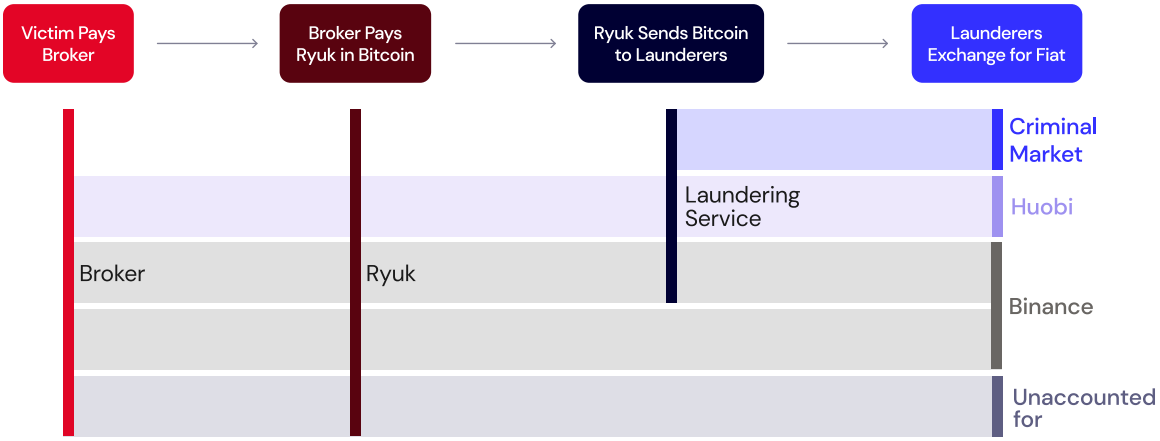
Source: Chainalysis.

22 https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/

Similarly, threat intel company, Advanced Intelligence, and cybersecurity firm, HYAS, tracked Bitcoin transactions to 61 addresses associated with the Ryuk syndicate. They estimate that the operator may be worth upwards of $150 million alone.[23] Their analysis sheds some light on how ransomware operators turn their exploits and the ransoms paid into usable cash.

Extorted funds are gathered in holding accounts, passed to money laundering services, then either funneled back into the criminal market and used to pay for other criminal services or cashed out at real cryptocurrency exchanges. The process follows these steps, as illustrated below:

- The victim pays a broker.
- The broker converts the cash into cryptocurrency.
- The broker pays the ransomware operator in cryptocurrency.
- The ransomware operator sends the cryptocurrency to a laundering service.
- The laundering service exchanges the coins for fiat currency on cryptocurrency exchanges like Binance and Huobi.



Source: AdvIntel.

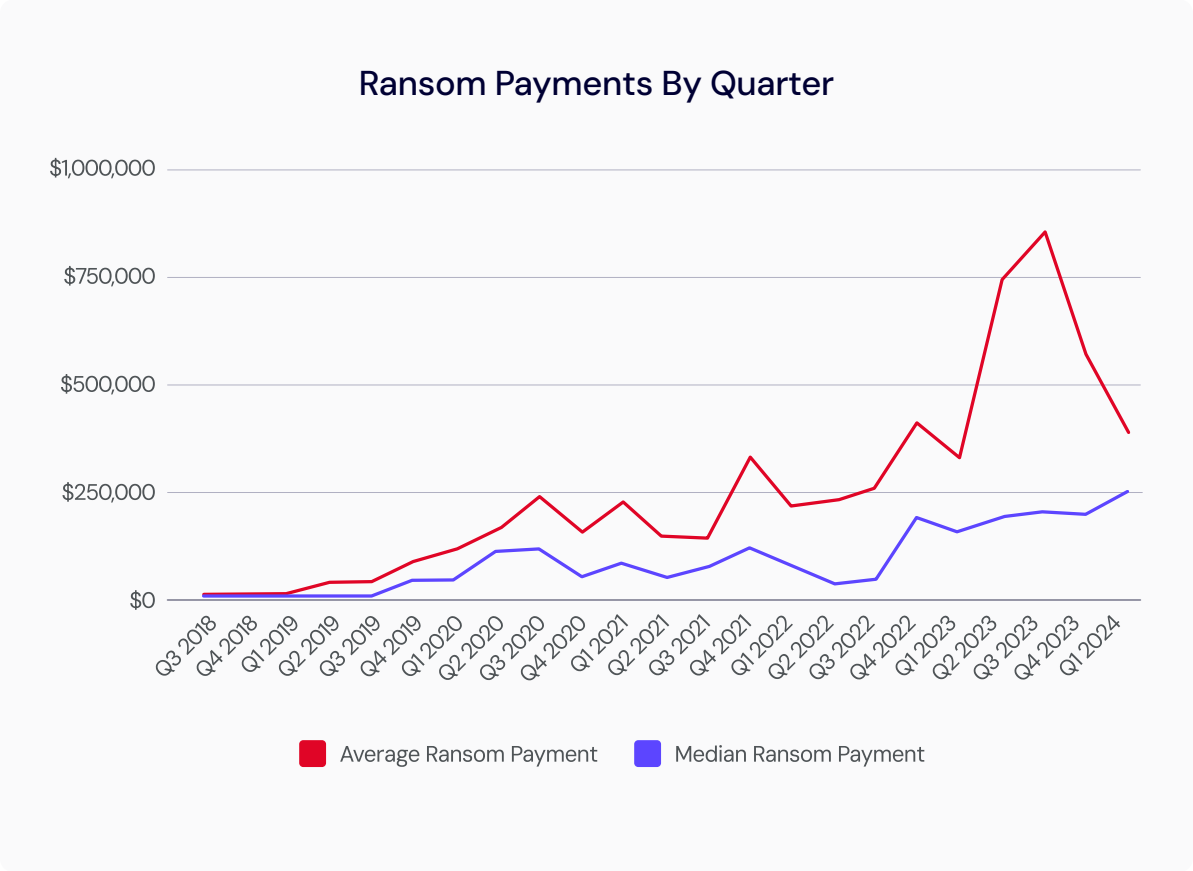
In an interesting development, the report found that Ryuk actually bypassed laundering services and cashed out some of their own cryptocurrency directly on exchanges using stolen identities—a brash move for any organized crime operation.

23 https://www.advanced-intel.com/post/crime-laundering-primer-inside-ryuk-crime-crypto-ledger-risky-asian-crypto-traders

The true cost of ransomware

Today, cybercriminals demand higher and higher ransoms on the order of hundreds of thousands or even millions of dollars. 2021 saw the highest ransom ever demanded hit $70 million in the REvil attack on Kaseya. But the ransoms themselves are just a portion, and often a small portion, of the overall cost of ransomware. This section describes the true cost and cost drivers of ransomware attacks to bring awareness to the financial risks associated with a ransomware attack.

The Sophos State of Ransomware 2024 report, a survey of 5,000 IT decision makers in mid-sized organizations in 14 countries, found the average payment was $2,000,000, up from $400,000 in 2023. However, the proportion of lower ransom payments has steadily decreased over the last three years, while the proportion of very high payments has soared[24] In their own reporting, Coveware found that the average ransom payment continued its downward trend from Q1 2024, decreasing 32% from Q4 2023 to $381,980.[25]



Source: Coveware.

Recent predictions from Cybersecurity Ventures paint an even bleaker picture, putting worldwide ransomware damages at $265 billion by the end of 2031.[26]

24 https://www.sophos.com/en-us/content/state-of-ransomware
25 https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024
26 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Global Ransomware Damage Costs*

2015: **$325 Million**

2017: **$5 Billion**

2021: **$20 Billion**

2024: **$42 Billion**

2026: **$71.5 Billion**

2028: **$157 Billion**

2031: **$265 Billion**

Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up every 11 seconds in 2021.

**Source: Cybersecurity Ventures*

Though the numbers vary, ransoms are not just pocket change for SMBs any way you slice it. But ransom payments are far from the only costs associated with ransomware attacks. The sensational ransom amounts may make headlines, but the true costs of ransomware recovery soar into the millions with the added complication of being much harder to quantify. The cost of recovery comes from a wide range of factors, including:

- Downtime.
- People hours.
- Stronger cybersecurity protections.
- Repeat attacks.
- Higher insurance premiums.
- Legal defense and settlements.
- Lost reputation.
- Lost business.

According to Sophos, the average bill for recovering from a ransomware attack, including downtime, people hours, device costs, network costs, lost opportunities, etc. was $2.73 million in 2024.[27] We'll dig into a few of these costs in more detail here.

- Downtime: The downtime resulting from ransomware can be incredibly disruptive, and not just for the companies themselves. As noted earlier, the Colonial Pipeline attack shut down gasoline service to almost half of the East Coast for six days. An attack on a Vermont health center had hospitals turning away patients. And an attack on Baltimore County Public Schools forced more than 100,000 students to miss classes. According to Veeam, the average downtime in 2023 amounted to over three weeks.[28] This time should be factored in when calculating the true cost of ransomware.
- People hours: While Colonial restored service after six days, CEO Joseph Blount testified before Congress more than a month after the attack that recovery was still ongoing. For a small business, most, if not all, of the company's efforts will be directed toward recovery for a period of time. Obviously, the IT team will be focused on getting systems back up and running, but other areas of the business will be monopolized as well. Marketing and communications teams will be tasked with crisis communications. The finance team will be brought into ransom negotiations. Human resources will be fielding employee questions and concerns. Calculating the total hours spent on recovery may not be possible, but it's a factor to consider in planning.
- Stronger cybersecurity protections: A company that's been attacked by ransomware will likely allocate more budget to avoid the same fate in the future, and rightfully so. Moreover, the increase in attacks and subsequent tightening of requirements from insurance providers means that more companies will be forced to bring systems up to speed in order to maintain coverage.[29]
- Repeat attacks: One of the cruel realities of being attacked by ransomware is that it makes businesses a target for repeat attacks. Unsurprisingly, cybercriminals don't always keep their promises when companies pay ransoms. In fact, paying ransoms lets cybercriminals know you're an easy mark. This behavior used to be rare, but has become more common.[30] We've seen reports of repeat attacks, either because companies already demonstrated willingness to pay or because the vulnerability that allowed cybercriminals access to systems remained susceptible to exploitation. More ransomware operators have been exfiltrating additional data during the recovery period, and copycat operators have been exploiting vulnerabilities that go unaddressed even for a few days. Some companies ended up paying a second time.[31]
- Higher insurance premiums: As more and more companies file claims for ransomware attacks and recoveries, insurers are increasing premiums. The damages their customers are incurring are beginning to exceed estimates, forcing premiums to rise.

27 https://www.sophos.com/en-us/content/state-of-ransomware
28 https://www.veeam.com/ransomware-trends-report-2023
29 https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
30 https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
31 https://www.zdnet.com/article/ransomware-this-is-the-first-thing-you-should-think-about-if-you-fall-victim-to-an-attack/

- Legal defense and settlements: When attacks affect consumers or customers, victims can expect to hear from the lawyers. Scripps Health, a San Diego hospital system, was hit with multiple class-action lawsuits after a ransomware attack in April 2021. And big box stores like Target and Home Depot both paid settlements in the tens of millions of dollars following breaches.[32] Even if your information security practices would hold up in court, for most companies, it's cheaper to settle than to suffer a protracted legal battle.
- Lost reputation and lost business: Thanks to the Colonial attack, ransomware is getting more coverage in the mainstream media. Hopefully this increased attention helps to discourage ransomware operators (they're not in it for the fame, and it's never a good day for cybercriminals when the president of the United States gets involved). But, that means companies are likely to be under more scrutiny if they happen to fall victim to an attack, jeopardizing their reputations and ability to develop business. And when companies lose their customers' trust, they lose money.

The increasing financial impact on businesses of all sizes has proven that the business of ransomware is booming with no signs of slowing down, and the cost of recovery is enough to put some ill prepared companies out of business.

32 https://www.washingtonpost.com/technology/2021/07/25/ransomware-class-action-lawsuit

How Ransomware Attacks Unfold

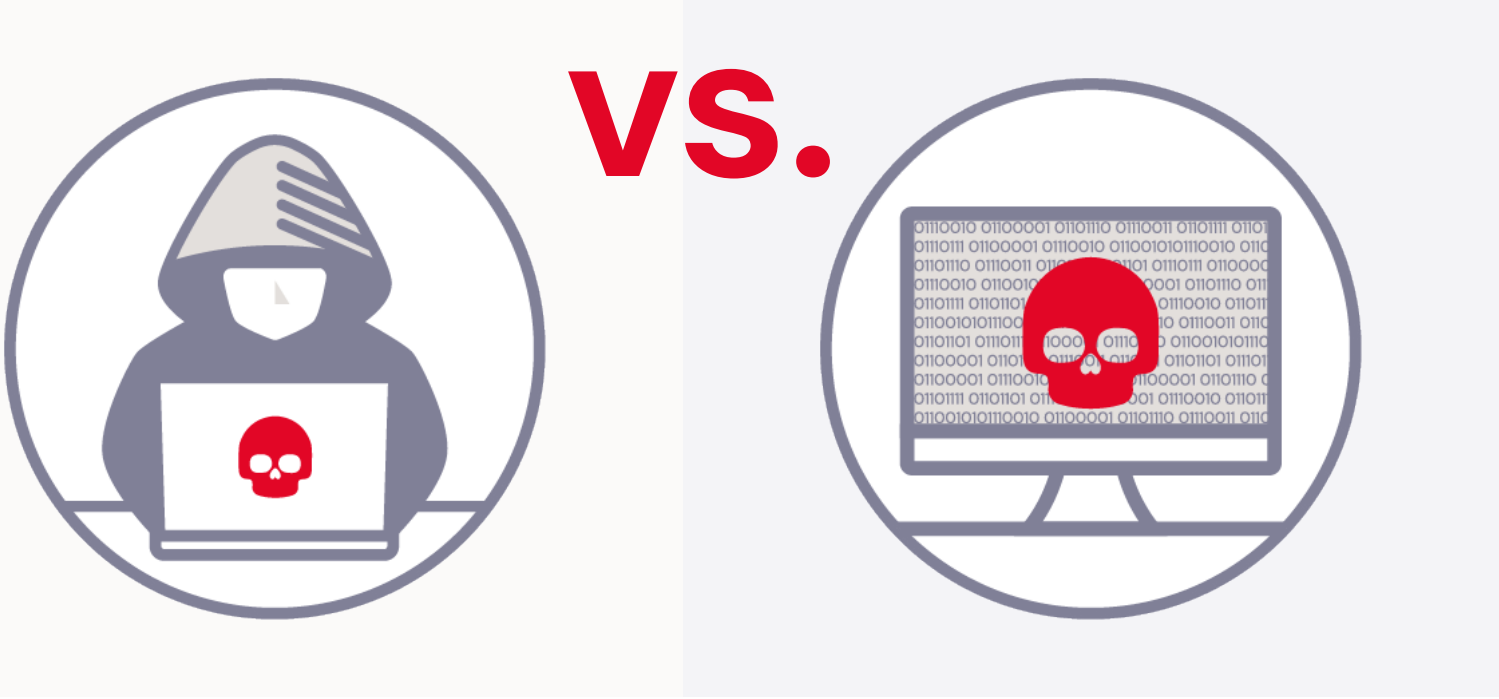
You can't respond to a ransomware attack without knowing how attacks happen in the first place. To prepare you to identify and respond to an attack, this section explains how ransomware enters your organization, describes the tools threat actors use to attack you, explains the steps in an attack, and highlights recent evolutions in attack techniques.

Attack vectors

Understanding how ransomware enters your systems can help you identify threats. One of the most important ransomware prevention best practices recommended by experts is to train staff on attack vectors and how to avoid them. This section describes the different ways ransomware enters your systems, so you can spot attacks before they wreak havoc.

Similar to the world of infectious diseases, ransomware infects a host through a "vector" or point of entry. Much like biological viruses enter a body through the lungs or bloodstream, ransomware can infect a business through different means.

A KnowBe4 report found that 91% of ransomware attacks start with a spear phishing email,[33] but that's far from the only method. Cybercriminals vary their tactics, and they continuously find new ways to infect victims, taking advantage of cultural, marketplace, and workforce distribution changes. There are two general types of ransomware attack vectors—human and machine.



33 https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email

Human attack vectors:

Cyber criminals like to exploit human factors—a tactic known as social engineering—to introduce viruses into a workplace through deception and manipulation. They prey on people's trust. Human attack vectors include:

- Phishing: Using fake emails to get people to click on a link or open a malware attachment.
- Spear phishing: Targeting employees with personal emails that appear to come from within an organization.
- SMSishing: Using fake text messages to get people to click on a link or provide personal information.
- Vishing: Leaving voicemails to trick people into installing malware on their devices to fix an imagined problem. (Yes, very convincing criminals will literally talk your staff into downloading ransomware.)
- Social media and instant messaging: Manipulating people into opening files infected with ransomware through social media posts or by hacking into instant messaging apps.

Machine attack vectors:

This type of vector is automated and doesn't directly involve human input or action. An employee may unknowingly trigger a download by visiting a website, for example, but their active participation is not required. Machine attack vectors include:

- Drive-by: Embedding a website with malicious code that automatically downloads when users visit, or "drive by," the site.
- Malvertising: Placing infected ads on search engines or social media sites that download malware when a user clicks on them.
- Remote desktop protocol (RDP) vulnerabilities: Using trial-and-error to guess user credentials or purchasing credentials on the black market to gain access to a system.
- System vulnerabilities: Studying a system, particularly when a system has not been updated with the latest security releases, to find ways to break in.
- Shared services vulnerabilities: Using file sharing or file sync services to spread viruses throughout an organization, employing automated sync to copy the virus over many machines in seconds.
- Network vulnerabilities: Exploiting poorly protected networks to spread viruses rapidly throughout an organization.

Tools of the rade

New ransomware variants pop up every day, but they generally fit into a few categories. This section describes the different kinds of ransomware and how they attack your business as well as other tools ransomware operators use to carry out attacks.

Once through a vector point, the ransomware locks every file it can using advanced encryption, effectively shutting a business down. It then demands payment, typically in Bitcoin, in exchange for decryption and restoration of normal operations. This type of approach, also known as cryptoware, may be the most common variety of ransomware, but it is far from the only one. Extortion-based variants are becoming more common. Types of ransomware, along with common ransomware brand names, include:

1. Cryptoware: This type of ransomware locks and encrypts files.[34, 35, 36]

- BOrOntOk
- Bad Rabbit
- Black Basta
- BlackCat (ALPHV)
- Cerber
- CryptoLocker
- CryptoWall
- Crysis
- CTB-Locker
- DarkSide
- Dharma Brrr
- Fair
- Jigsaw
- KeRanger
- Locky
- Mado
- Medusa
- Rhysida
- Ryuk
- Shade/Troldesh
- Spider
- TeslaCrypt
- TorrentLocker
- WannaCry
- ZCryptor

2. Non-encrypting viruses: These lock screens restrict file access without encrypting files.

- Reveton/Police Trojan[37]

3. Master boot record (MBR) encryption: This variant encrypts only the MBR or Microsoft's NTFS and prevents local devices from booting up in a live OS environment.

- GoldenEye[38]
- Humble[39]
- Petya and NotPetya[40]

4. Extortionware or leakware: This ransomware threatens to expose sensitive or confidential data unless a ransom is paid.[41]

- Avaddon
- Ako
- CLoP
- Conti
- DarkSide
- DoppelPaymer
- Egregor
- Everest
- Kupidon
- Lockbit
- Light
- Maze
- Mespinoza
- MountLocker
- Netfilim
- Netwalker
- Pay2Key
- Ragnarok
- RagnarLocker
- RansomeEXX
- REvil
- Suncrypt

5. Mobile device ransomware: This type of virus targets cell phones using drive-by downloads or fake app downloads.[42, 43]

- CryptoLocker
- Doublelocker
- ScarePakage
- Android.Locker.38.origin
- Worm.Koler

34 https://usa.kaspersky.com/resource-center/threats/ransomware-attacks-and-types
35 https://www.datto.com/blog/common-types-of-ransomware
36 https://en.wikipedia.org/wiki/Ransomware
37 https://www.sdxcentral.com/security/definitions/case-study-reveton-ransomware/
38 https://www.datto.com/blog/common-types-of-ransomware
39 https://www.zdnet.com/article/these-two-unusual-versions-of-ransomware-tell-us-a-lot-about-how-attacks-are-evolving/
40 https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html
41 https://www.cisecurity.org/blog/ransomware-the-data-exfiltration-and-double-extortion-trends/
42 https://us.norton.com/internetsecurity-mobile-what-is-mobile-ransomware.html
43 https://blog.knowbe4.com/evolution-of-mobile-ransomware

Some of the brands listed above are targeted at consumers. It's also important to note that larger ransomware operators carry out bespoke attacks, meaning they don't use known ransomware variants, making them much harder to detect and recover from.

In addition to ransomware variants, cybercriminals use other tools in carrying out their attacks. Other tools of the trade include:

- Exploit kits: These software kits automatically exploit vulnerabilities on victims' laptops and desktops without being detected. Because they are automated, they've become popular as a way to deploy malware in a "spray and pray" method, hoping for a hit.[44]
- Spyware: This software monitors a computer or network to collect information without consent. Criminal groups use this to find usernames and passwords.[45]
- Botnets: Botnets are a network of computers controlled by a botmaster using malware. Cybercriminals use these to carry out malicious actions across a wide network of machines.[46]

Attack progression

Here, we'll explain how a ransomware attack progresses from infection through payment or recovery so you know what to expect if you're ever attacked.

A typical ransomware attack follows the following phases:

1. Infection: The ransomware enters through a vector, like a phishing email or attachment, and initiates an install on the endpoint and any available, networked devices.
2. Secure key exchange: The ransomware alerts the cybercriminal's command and control server to create cryptographic keys for use on the local network.
3. Encryption: The ransomware encrypts files on the local devices and network.
4. Extortion: The ransomware displays instructions on local device screens demanding the organization make ransom payments or risk destruction of the data.
5. Payment or recovery: The organization has two choices at this point. (1) They can pay the ransom and rely on the cybercriminals to restore encrypted files—far from a guarantee. (2) They can delete infected files and restore data from a clean backup.

These days many ransomware attacks are focused on a given organization or business, most likely an SMB. To accomplish this targeting, an attacker will research their prey looking for avenues into the organization's internal networks and beyond. For example, employees of the company might receive a phishing email purported to be from the CEO asking for access to an internal system. Or an attacker could launch a general phishing attack hoping to gain access to a couple of user accounts, thus allowing them to exploit their newfound access to the company. The attacker could also take a shortcut and purchase compromised credentials for their target company on the dark web. All of this is done so that during the infection phase the attacker can target the systems and servers required to disable the business or organization, when the time comes.

44 https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit
45 https://www.paloaltonetworks.com/cyberpedia/what-is-spyware
46 https://www.paloaltonetworks.com/cyberpedia/what-is-botnet

Twists on attack techniques

Cybercriminals are constantly evolving to and developing new ways of threatening businesses. This section describes three emerging trends in their attack methods including exfiltration, attacking backups, and disinformation campaigns.

Exfiltration: The Maze ransomware syndicate carried out the first high-profile exfiltration attacks in 2019.[47, 48] Since then, more and more attackers are going beyond just locking and encrypting files to exfiltrating or extracting sensitive data from their victims, which they use to extort victims. Coveware reported that 77% of ransomware attacks in Q1 2021 involved extortion or the threat to leak stolen data, up 7% from Q4 2020.[49]

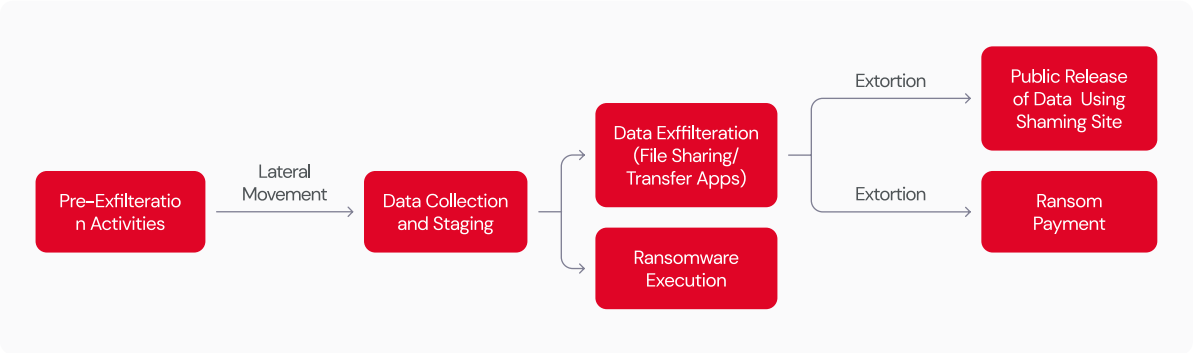
In exfiltration attacks, cybercriminals attempt to:

- Extract the most easily accessible sensitive information.
- Deploy encrypting ransomware to as much of the network as possible.

Rather than attempting to sell this data to the highest bidder—a time and resource intensive task—most cybercriminals use the stolen data to prove the attack happened and to threaten a leak, thus compelling payment of the ransom. The threat of leaking data is often sufficient to require companies that handle sensitive information to pay out of a legal obligation.

The exfiltration process:

- Pre-exfiltration Activities: Threat actors establish access and identify systems that may be storing sensitive data.
- Data Collection and Staging: Threat actors prepare files to be exfiltrated.
- Data Exfiltration: Threat actors use a file transfer method to exfiltrate data.
- Ransomware Execution: Once the files have been exfiltrated, the threat actor will execute the ransomware encryption.
- Extortion: The threat actor either threatens to leak data unless they pay the ransom, or they actually leak the data, posting it to an extortion site, and require payment to have the data taken down.



Source: Palo Alto Networks.[50]

47 https://www.infosecurity-magazine.com/news/maze-exfiltration-tactic-widely
48 https://www.canadianlawyermag.com/practice-areas/privacy-and-data/cyber-attacks-more-sophisticated-data-exfiltration-not-going-away-risk-expert/356810
49 https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
50 https://www.crypsisgroup.com/insights/ransomwares-new-trend-exfiltration-and-extortion

Public sector entities are frequent targets of exfiltration attacks because they store personally identifiable information (PII) like social security numbers and health information.[51] For example, the Conti syndicate posted nearly 26,000 files from the Broward County School District after they refused to pay the $40 million ransom.[52] Cybercriminals leaked sensitive information from the Washington, D.C. Metropolitan Police Department including officers' records, financials, and background check information as well as documents that described security information related to the January 2021 attack on the Capitol.[53]

Backup storage attacks: Backups are supposed to be a failsafe for ransomware, but any system that's online and connected to a network is ripe for encryption. Cybercriminals are going after backups because they don't stand to get paid if their victims can simply restore their systems. Attacks on backup data are increasing for a few reasons:

- Expanding attack surfaces (more data across more products) give cybercriminals more opportunity to access backup copies.[54]
- Cybercriminals know SMBs and the public sector may not have as robust backup and recovery plans as large enterprises.

Variants like WannaCry, Locky, Cryptolocker, and CryptXXX are all capable of deleting backups, making the resulting recoveries all the more challenging.[55] For example, it took UnitingCare Queensland two months to recover from a ransomware attack by the REvil/Sodinokibi syndicate that attempted to delete backups.[56, 57]

Disinformation campaigns: Former U.S. cybersecurity head Chris Krebs explained to Axios that some nefarious organizations are even offering "disinformation as a service" where they launch a viral negative publicity attack against a business for a fee. While not a type of ransomware, specifically, these attacks constitute a new weapon on the menu right next to ransomware for criminals looking to disrupt business operations. Businesses have little legal recourse available to them as disinformation campaigns are not illegal. The best course of action in the event of a disinformation campaign is prevention. Start by identifying potential areas where your business could be attacked and developing a clear protocol for responding.[58]

51 https://www.cisecurity.org/blog/ransomware-the-data-exfiltration-and-double-extortion-trends/
52 https://www.sun-sentinel.com/news/education/fl-ne-broward-schools-hackers-post-files-20210419-mypt2qtlc5a7xela4x6bcg5hdy-story.html
53 https://apnews.com/article/police-technology-government-and-politics-1aedfcf42a8dc2b004ef610d0b57edb9
54 https://www.cohesity.com/resource-assets/tip-sheet/5-ways-ransomware-attacks-backup-and-how-you-can-prevent-it-tip-sheet-en.pdf
55 https://www.unitrends.com/blog/will-ransomware-start-targeting-enterprise-backups
56 https://www.lexology.com/library/detail.aspx?g=4ff23362-6dd3-4d6a-823a-4552b77827be
57 https://www.itnews.com.au/news/unitingcare-queensland-confirms-revil-ransomware-infection-564215
58 https://www.axios.com/disinformation-business-security-a71b7758-cba5-49ce-844d-b5e70a1c65b2.html

Protecting Your Business From Ransomware

There's a reason ransomware attacks continue to wreak havoc for large and small businesses alike—they are more and more profitable and implementation is easier as well. Unfortunately, 50% of IT professionals don't feel they're prepared for a ransomware attack.[59] With that in mind, what is the best way to protect your business? This section describes best practices in ransomware prevention, emerging tools like Object Lock that enhance ransomware protection with immutability, evolving backup strategies, steps for responding to a ransomware attack, and recommendations for recovery planning. Consider this your ransomware prevention and response playbook.

Best practices in ransomware prevention

The old saying, "an ounce of prevention is worth a pound of cure" could not be more applicable when it comes to ransomware. Rather than stockpiling cash in the event of an attack, spend that money on prevention—it's the most pragmatic protection to implement. Security experts suggest several precautionary measures for preventing a ransomware attack, including:

1. Use antivirus and anti-malware software or other security policies to block known payloads from launching.
2. Make frequent, comprehensive backups of all important files and isolate them from local and open networks. Immutable backup options such as Object Lock offer users a way to maintain truly air-gapped backups. The data is fixed, unchangeable, and cannot be deleted within the time frame set by the end user. With immutability set on critical data, you can quickly restore uninfected data from your immutable backups, deploy them, and return to business without interruption.
3. Keep offline backups of data stored in locations inaccessible from any potentially infected computer, such as disconnected external storage drives or the cloud, which prevents them from being accessed by the ransomware.
4. Install the latest security updates issued by software vendors of your OS and applications. Remember to patch early and patch often to close known vulnerabilities in operating systems, browsers, and web plugins.
5. Consider deploying security software to protect endpoints, email servers, and network systems from infection.

59 https://purplesec.us/resources/cyber-security-statistics/

6. Exercise cyber hygiene, such as using caution when opening email attachments and links.
7. Segment your networks to keep critical computers isolated and to prevent the spread of malware in case of attack. Turn off unneeded network shares.
8. Turn off admin rights for users who don't require them. Give users the lowest system permissions they need to do their work.
9. Restrict write permissions on file servers as much as possible.
10. Educate yourself and your employees in best practices to keep malware out of your systems. Invest in training for employees on how to recognize phishing scams and human engineering aimed at turning victims into abettors. Human vectors are the most frequently used points of entry for ransomware, and training employees to identify and report suspicious emails, websites, ads, messages, and phone calls is still one of the most effective methods to avoid ransomware attacks.

The best way to respond to a ransomware attack is to avoid having one in the first place. Other than that, making sure your valuable data is backed up and unreachable by a ransomware infection will ensure that your downtime and data loss will be minimal or none if you ever suffer an attack.

Object Lock and immutability

As cybercriminals increasingly target companies' backups in addition to their production data, more robust backup protection tools are evolving to meet the threat. Object Lock is one of those tools. This section explains the enhanced protection Object Lock offers by storing data with immutability.

Object Lock is a powerful backup protection tool that prevents a file from being altered or deleted until a given date. It allows you to store objects using a Write Once, Read Many (WORM) model, meaning after it's written, data cannot be modified or deleted for a defined period of time. Any attempts to manipulate, copy, encrypt, change, or delete the file will fail during that time. The files may be accessed, but no one can change them, including the file owner or whoever set the Object Lock and—most importantly—any cybercriminal that happens upon the credentials of that person.

Using Object Lock to protect your data means no one—not cybercriminal, not ransomware viruses, not even you—can edit or delete your files. It creates a virtual air gap similar to the physical air gap that LTO tape provides. With tape, your backup copies are protected from viruses and ransomware by a literal gap of air—they're stored on a shelf somewhere and not connected to a network. Object Lock creates an air gap, but it all happens in the cloud.

In the event of a ransomware attack, you don't want to worry about whether or not your backups are safe. Knowing you can easily restore your data from immutable backups created prior to an attack helps ensure you can avoid downtime, minimize productivity disruptions, and easily and quickly resume normal operations.

Only a few storage platforms currently offer the feature, but if your provider is one of them, you can enable Object Lock and specify the length of time an object should be locked in the storage provider's user interface or by using API calls.

Backup strategies: 3-2-1 vs. 3-2-1-1-0 vs. 4-3-2

The gold standard until recently has been the 3-2-1 backup rule—three copies of your data on two different media with one copy stored off-site. The 3-2-1 rule still has value, especially for individuals who aren't backing up at all. But today, the gold standard is evolving. This section introduces emerging strategies that offer more protection from ransomware than 3-2-1 in the cloud era.

While a 3-2-1 strategy with off-site copies stored in the cloud works well for events like a natural disaster or accidental deletion, it lost the air gap protection that tape backups once provided—there was literally a gap of air between the tapes and the network. They're not as catchy as 3-2-1, but strategies like 3-2-1-1-0 and 4-3-2 offer more protection in the era of cloud backups and ransomware.

What is 3-2-1-1-0?

A 3-2-1-1-0 strategy stipulates that you:

- Maintain at least three copies of business data.
- Store data on at least two different types of storage media.
- Keep one copy of the backups in an off-site location.
- Keep one copy of the media offline or air gapped.
- Ensure all recoverability solutions have zero errors.

The 3-2-1-1-0 method reintroduces the idea of an offline or air-gapped copy—either tape backups stored off-site as originally intended in 3-2-1, or cloud backups stored with immutability, meaning the data cannot be modified or changed.

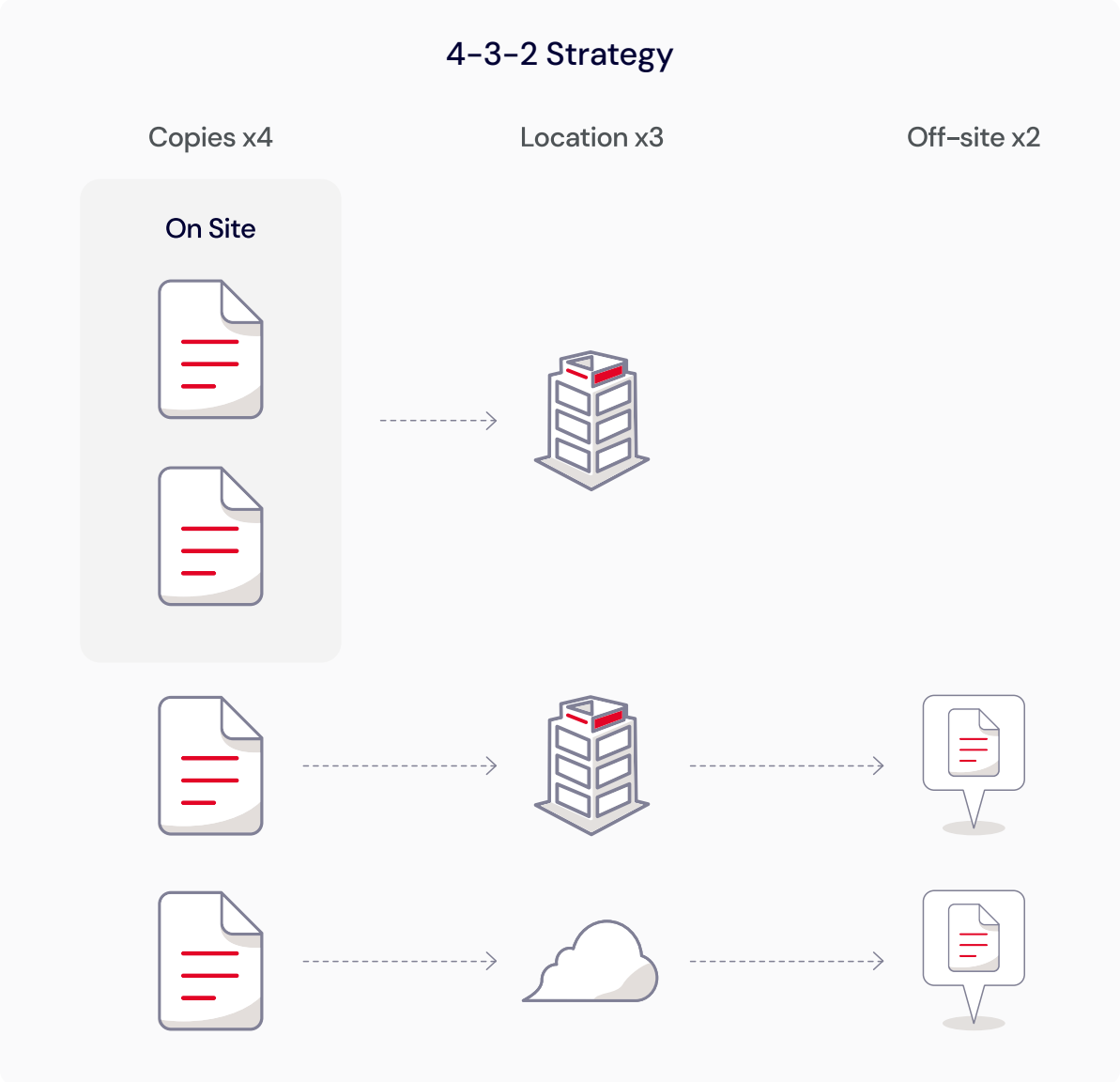
The 3-2-1-1-0 strategy goes a step further to require that backups are stored with zero errors. This includes monitoring data on a daily basis, correcting for any errors as soon as they're identified, and regularly performing restore tests. A strategy like 3-2-1-1-0 offers the protection of air-gapped backups with the added fidelity of more rigorous monitoring and testing.

What is 4-3-2?

If your data is being managed by a disaster recovery expert, your backups may be subscribing to the 4-3-2 rule:

- Four copies of your data.
- Data in three locations (on-prem with you, on-prem with a managed service provider, and stored with a cloud provider).
- Two locations for your data are off-site.

A 4-3-2 strategy means backups are duplicated and geographically distant to offer protection from events like natural disasters. Backups are also stored on two separate networks, isolating them from production networks in the event they're compromised. Finally, backup copies are stored with immutability, protecting them from deletion or encryption should a cybercriminal gain access to systems.



How to respond to a ransomware attack

So, you've been attacked by ransomware. What should you do next? Here, we'll walk through recommended steps for responding to a ransomware attack, including:

1. Isolate the infection: Prevent the infection from spreading by separating all infected computers from each other, shared storage, and the network.
2. Identify the infection: From messages, evidence on the computer, and identification tools, determine which malware strain you are dealing with.
3. Report: Report to the authorities to support and coordinate measures to counter attack.
4. Determine your options: You have a number of ways to deal with the infection. Determine which approach is best for you.
5. Restore and refresh: Use safe backups and program and software sources to restore your systems or outfit a new platform.
6. Plan to prevent recurrence: Make an assessment of how the infection occurred and what you can do to put measures into place that will prevent it from happening again.

1. Isolate the infection

The rate and speed of ransomware detection is critical in combating fast moving attacks before they succeed in spreading across networks and encrypting vital data.

The first thing to do when a computer is suspected of being infected is to isolate it from other computers and storage devices. Disconnect it from the network (both wired and Wi-Fi) and from any external storage devices. Cryptoworms actively seek out connections and other computers, so you want to prevent that from happening. You also don't want the ransomware communicating across the network with its command and control center.

Be aware that there may be more than just one patient zero, meaning that the ransomware may have entered your organization through multiple computers, or may be dormant and not yet have shown itself on some systems. Treat all connected and networked computers with suspicion and apply measures to ensure that all systems are not infected.

2. Identify the infection

Most often the ransomware will identify itself when it asks for ransom. There are numerous sites that help you identify ransomware, including ID Ransomware.[60] The No More Ransom! Project[61] provides the Crypto Sheriff[62] to help identify ransomware.

Identifying the ransomware will help you understand what type of ransomware you have, how it propagates, what types of files it encrypts, and maybe what your options are for removal and disinfection. It also will enable you to report the attack to the authorities, which is recommended.

60 https://id-ransomware.malwarehunterteam.com/index.php
61 https://www.nomoreransom.org/en/index.html
62 https://www.nomoreransom.org/crypto-sheriff.php?lang=en

3. Report to the authorities

You'll be doing everyone a favor by reporting all ransomware attacks to the authorities. The FBI urges ransomware victims to report ransomware incidents regardless of the outcome. Victim reporting provides law enforcement with a greater understanding of the threat, provides justification for ransomware investigations, and contributes relevant information to ongoing ransomware cases. Knowing more about victims and their experiences with ransomware will help the FBI to determine who is behind the attacks and how they are identifying or targeting victims.

You can file a report with the FBI at the Internet Crime Complaint Center.[63]

4. Determine your options

Your options when infected with ransomware are:

- To pay the ransom.
- To try to remove the malware.
- To wipe the system(s) and reinstall from scratch.

Unfortunately, paying the ransom doesn't always lead to decryption—42% of organizations that paid ransoms did not end up getting their files back.[64] Criminals emboldened by this trend have become such a concern that the FBI issued a public service announcement in late 2019 urging victims not to negotiate or pay ransoms.[65] In fact, in a number of countries, it may be illegal to make ransomware payments.

Paying the ransom encourages more ransomware, and in many cases the unlocking of the encrypted files is not successful. Even if you decide to pay, it's very possible you won't get back your data.

That leaves two other options: removing the malware and selectively restoring your system, or wiping everything and installing from scratch.

5. Restore or start fresh

You have the choice of trying to remove the malware from your systems or wiping your systems and reinstalling from safe backups and clean OS and application sources.

Remove the malware: There are internet sites and software packages that claim to be able to remove ransomware from systems. The No More Ransom! Project[66] is one. Other options can be found as well.[67] Whether you can successfully and completely remove an infection is up for debate. A working decryptor doesn't exist for every known ransomware, and unfortunately it's true that the newer the ransomware, the more sophisticated it's likely to be and the less time the good guys have had to develop a decryptor.

63 https://www.ic3.gov/default.aspx
64 https://tmt.knect365.com/uploads/DCK-datacenter-ransomware-guide2019-9afd99804b7529633e4a7d8972eb86f2.pdf
65 https://www.ic3.gov/Media/Y2019/PSA191002
66 https://www.nomoreransom.org/en/index.html
67 https://www.quora.com/How-do-I-recover-my-files-after-Ransomware-attack

Wipe all systems completely: The surest way of being certain that malware or ransomware has been removed from a system is to do a complete wipe of all storage devices and reinstall everything from scratch. Formatting the hard disks in your system will ensure that no remnants of the malware remain. If you've been following a sound backup strategy, you should have copies of all your documents, media, and important files right up to the time of the infection.

Be sure to determine the date of infection as well as you can from malware file dates, messages, and other information you have uncovered about how your particular malware operates. Consider that an infection might have been dormant in your system for a while before it activated and made significant changes to your system. Identifying and learning about the particular malware that attacked your systems will enable you to understand how that malware functions and what your best strategy should be for restoring your systems.

Select a backup or backups that were made prior to the date of the initial ransomware infection. If you've been following a good backup policy with both local and off-site backups, you should be able to use backup copies that you are sure were not connected to your network after the time of attack and hence protected from infection. Backup drives that were completely disconnected should be safe, as are files stored in the cloud with immutability.

You'll need to reinstall your OS and software applications from the source media or the internet. If you've been managing your account and software credentials in a sound manner, you should be able to reactivate accounts for applications that require it. If you use a password manager to store your account numbers, usernames, passwords, and other essential information, you can access that information through their web interface or mobile applications. You just need to be sure that you still know your master username and password to obtain access to these programs. It's also a good idea to begin changing all your passwords to help prevent further attacks.

Disaster recovery and business continuity

Backup is vital as part of a disaster recovery plan, but the actual "recovery"—how you get your business back online using that backup data—is just as important. This section provides some recommendations for enhancing your disaster recovery efforts.

If you have solid, immutable backups, you will be able to restore operations, but the effort it takes to actually recover all of your systems from your backups is not as straightforward or speedy as you may think. Few businesses can survive the hit of weeks or months spent offline.

To avoid that fate, there are a couple steps you can take to make your recovery more resilient:

1. Develop a recovery plan: Maybe your backup system is well-established, but the lift of recovery planning is overshadowed by more immediate demands on your team when you're already stretched too thin. Or maybe you've looked into disaster recovery as a service (DRaaS) solutions, but they're not right-sized for your business. Either way, developing this incredibly important plan is critical to your business. A good recovery plan should include:
    - A business impact analysis that identifies risks and responses in the event of an attack and contingencies for different kinds of attacks.
    - A set of recovery procedures to restore operations.
    - An identified response team and specific roles.
    - Documentation of your backup plan.
    - Training procedures for implementing the plan.
    - A schedule for regular updates to the plan.

2. Institute regular testing of your recovery plan: Go through the process of recovering from your backups at least once a year, if not more. Like a fire drill, practicing the protocols your team will need to use in the event of a disaster keeps them top of mind and prevents chaos and confusion if the real thing were to happen. Bring in users of your system to verify that data has been restored.

DRaaS providers can advise you on the above and often include service level agreements for how fast they can get your business back up and running. Depending on your industry, banking and finance for example, trusting your recovery to the professionals might be preferred.

For businesses in industries that handle less sensitive information, disaster recovery and business continuity planning can be done independently using tools like Terraform, an infrastructure as code provider, and Ansible, an open-source configuration management tool, to spin up servers on bare metal cloud providers on demand. For savvy IT teams, this is an incredibly small amount of work to architect a recovery plan. When disaster strikes, teams can run the code to quickly bring up an orchestrated combination of on-demand servers, firewalls, networking, storage, and other infrastructure. The code then pulls across the backup data to get the business back online as soon as possible.

This is profound on two fronts: First, these code packages are free and are relatively easily modified to suit your preferred providers. Second, they offer the dependability of on-call compute resources without having to pay for them until they're 100% necessary. It's like insurance you can buy after you get in a car wreck.

Whether you choose to handle disaster recovery on your own or outsource it to professionals, don't put it off any longer. Any plan is better than none at all.

Conclusion

From this paper, the conclusions should be twofold. First, ransomware attacks are here to stay, so preventing and responding to them will become an increasingly critical aspect of IT workloads. Second, and more important, there are simple steps you can take today to massively reduce your workload in this area when disaster strikes:

- Follow ransomware prevention best practices.
- Ensure your backup strategy is compliant with 3-2-1, if not a more comprehensive method like 3-2-1-1-0 or 4-3-2.
- Consider air-gapped backups using cloud storage and immutability. Testing these solutions with any range of services is easy, and once you choose one, you'll rest easy, too, knowing that your data is safely tucked away from any malicious code or actors.
- Develop a disaster recovery and business continuity plan so you're not caught off guard in the event of a ransomware attack.