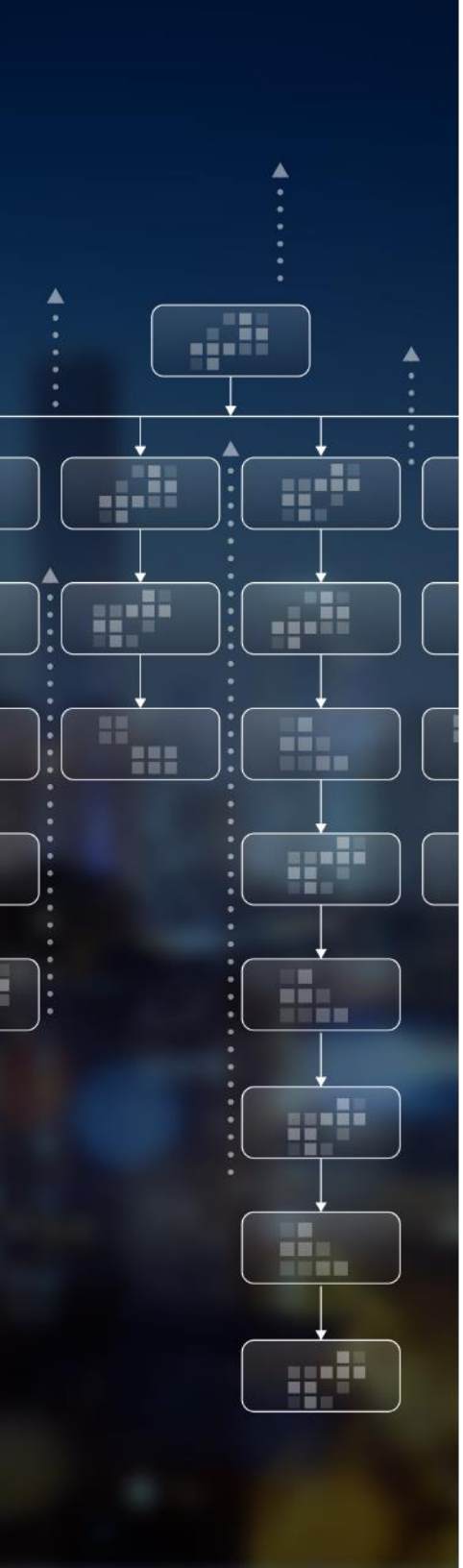


What is ransomware? How it works and how to remove it

March 2024

TechTarget

In this guide:

Ransomware is malware that locks and encrypts a victim's data, files, devices or systems, rendering them inaccessible and unusable until the attacker receives a ransom payment. A ransomware attack can shut down a business for days, even weeks and -- even when the company pays the ransom -- there's no guarantee it will ever get its assets back, or that it won't be attacked again. This guide covers the history and basics of ransomware, identifies the most common targets and offers expert instructions on how to prevent an attack. Or, if the worst happens, how to recognize an attack's taken place and remove the ransomware as swiftly as possible.

In this guide:

What is ransomware? How it works and how to remove it

SHARON SHEA, EXECUTIVE EDITOR

The first iterations of ransomware used only encryption to prevent victims from accessing their files and systems. Victims that had regular backups were able to restore their data, however, negating the need to pay a ransom. In turn, malicious actors began to incorporate cyber extortion tactics, using additional threats to blackmail victims into making ransom payments. Also, attackers started increasingly targeting victims' backups to prevent organizations from restoring their data. Veeam's "2023 Ransomware Trends Report" found more than 93% of ransomware attacks the previous year specifically targeted backup data.

Malware is the umbrella term for any malicious software that enables unauthorized access to a user's systems. Ransomware is a subset of malware that demands payment to unlock and decrypt the data, enabling the victim to regain access.

Ransomware can be devastating to individuals, organizations and even entire municipalities or countries. Because they continue to be successful, these financially motivated attacks are becoming increasingly common. Verizon's "2023 Data Breach Investigations Report" found ransomware was involved in 24% of all breaches, and Sophos' "The State of Ransomware 2023" reported 66% of organizations

In this guide:

experienced a ransomware attack in the past year, with 76% of those attacks resulting in data encryption.

HOW DOES RANSOMWARE WORK?

The ransomware lifecycle has six general stages: malware distribution and infection; command and control; discovery and lateral movement; malicious theft and file encryption; extortion; and resolution.

STAGE 1: MALWARE DISTRIBUTION AND INFECTION

Before attackers can demand a ransom, they must infiltrate their victims' systems and infect them with malware. The most common ransomware attack vectors are phishing, Remote Desktop Protocol (RDP) and credential abuse, and exploitable software vulnerabilities:

- **Phishing.** This is the most popular type of social engineering, and it continues to be the top attack vector for all types of malware. Attackers lace legitimate-looking emails with malicious links and attachments to trick users into unwittingly installing malware. Smishing, vishing, spear phishing and watering hole attacks are all forms of phishing and social engineering scams attackers use to deceive people into initiating malware installation.
- **RDP and credential abuse.** This involves the use of brute-force or credential-stuffing attacks or the purchase of credentials off the dark web, with the goal of

In this guide:

logging into systems as legitimate users, then infecting the network with malware. RDP, a favorite of attackers, is a protocol that enables administrators to access servers and desktops from virtually anywhere and lets users remotely access their desktops. Improperly secured RDP implementations, however, are a common ransomware entry point.

- **Software vulnerabilities.** These are also a frequent target for ransomware infections. Attackers infiltrate a victim's systems by attacking unpatched or out-of-date software. One of the biggest ransomware incidents in history, WannaCry, is linked to the EternalBlue exploit, a vulnerability in unpatched versions of the Windows Server Message Block (SMB) protocol.

STAGE 2: COMMAND AND CONTROL

A command-and-control (C&C) server set up and operated by the ransomware attackers sends encryption keys to the target system, installs additional malware and facilitates other stages of the ransomware lifecycle.

STAGE 3: DISCOVERY AND LATERAL MOVEMENT

This two-step stage involves attackers first gathering information about the victim network to help them better understand how to launch a successful attack, and then spreading the infection to other devices and elevating their access privileges to seek out valuable data.

In this guide:

STAGE 4: MALICIOUS THEFT AND FILE ENCRYPTION

In this stage, attackers exfiltrate data to the C&C server to use in extortion attacks down the line. Attackers then encrypt the data and systems using the keys sent from their C&C server.

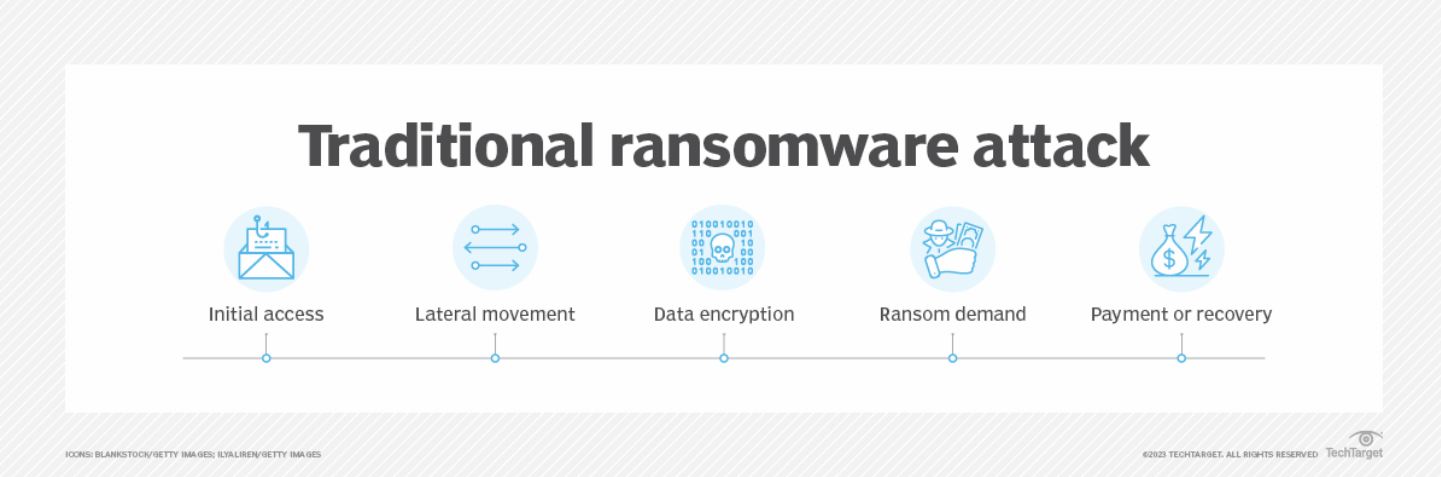
STAGE 5: EXTORTION

The attackers demand a ransom payment. The organization now knows it is a victim of a ransomware attack.

STAGE 6: RESOLUTION

The victim organization must go into action to address and recover from the attack. This could involve restoring backups, implementing a ransomware recovery plan, paying the ransom, negotiating with attackers or rebuilding systems from the ground up.

In this guide:



WHAT ARE THE DIFFERENT TYPES OF RANSOMWARE?

Ransomware is defined and categorized by how it is delivered and what it impacts. Delivery includes ransomware as a service (RaaS), automated delivery (not as a service) and human-operated delivery. The impact could be data unavailability, data destruction, data deletion, and data exfiltration and extortion.

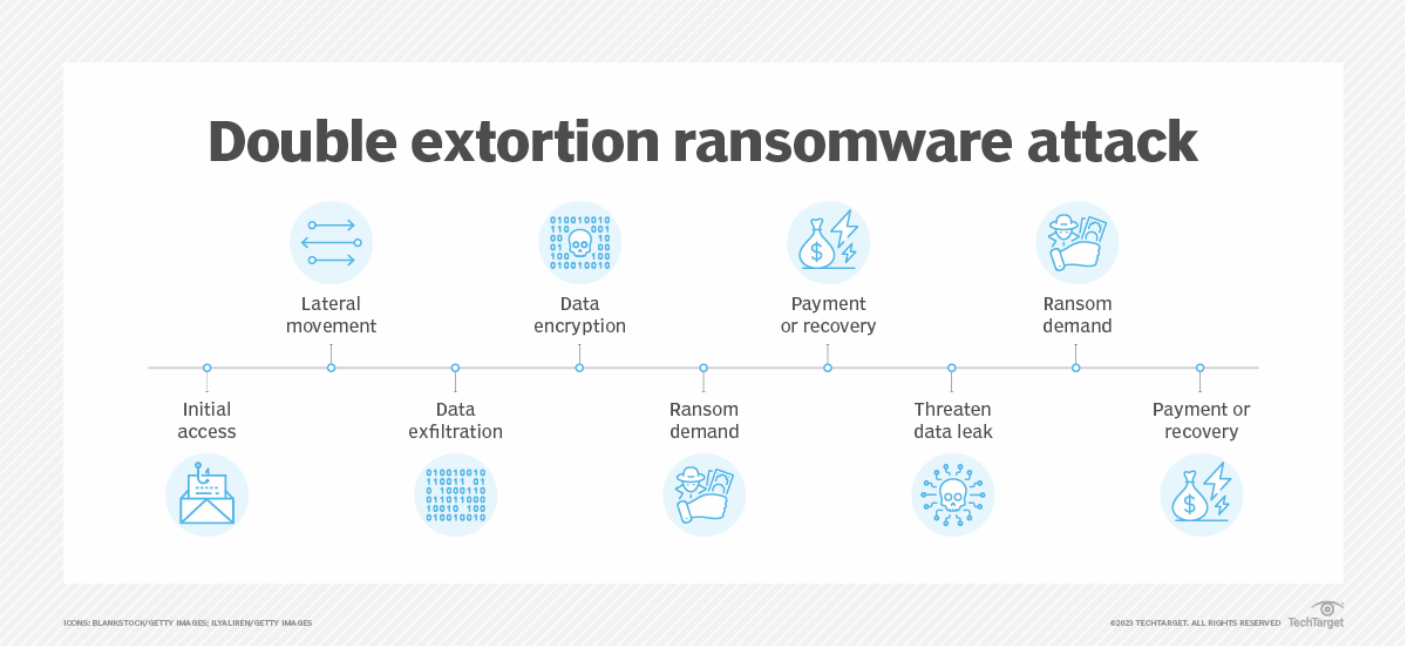
The following terms further describe the different types of ransomware:

- Locker ransomware locks victims out of their data or systems entirely.
- Crypto ransomware encrypts all or some of victims' files.

In this guide:

- Scareware scares victims into believing their devices are infected with ransomware when they might not be. Attackers then trick victims into buying software that will purportedly remove the ransomware when it actually steals data or downloads additional malware.
- Extortionware, also known as *leakware*, *doxware* and *exfiltrationware*, involves attackers stealing victims' data and threatening to make it public or sell it on the dark web.
- Wiper malware acts like ransomware but in reality is a destructive form of malware that erases data from victims' systems, even if they make ransom payments.
- Double extortion ransomware encrypts victims' data and exfiltrates data to extort victims into paying a ransom, potentially twice.
- Triple extortion ransomware encrypts victims' data, exfiltrates data to extort victims and adds a third threat. Often, this third vector is a DDoS attack or the extortion of the victims' customers, partners, suppliers and stakeholders into paying ransoms or urging the initially infected organization to pay. This could result in attackers receiving three or more ransom payments for a single attack.
- RaaS, a delivery model rather than type of ransomware, is often included in types of ransomware lists. RaaS is a subscription-based model in which ransomware developers sell the pay-for-use malware to ransomware operators, who give the developers a percentage of the attack profits.

In this guide:



WHAT ARE THE EFFECTS OF RANSOMWARE ON BUSINESSES?

Depending on the attack's sophistication, the attacker's motivation and the victim's defenses, the consequences of ransomware can range from minor inconvenience to expensive and painful recovery to complete devastation.

When people hear, "We've been hit with ransomware," their minds usually turn to the amount of the ransom demand. The Sophos survey found the average ransomware payment in 2023 was $1.54 million, up from $812,380 the previous year.

In this guide:

Should an organization pay the ransom?

Cybersecurity experts and government authorities discourage individuals and organizations from paying ransoms. Some businesses choose to pay, however, often in hope of recovering and regaining access to their sensitive data faster. Experts argue that paying ransoms encourages attackers, puts targets on victims' backs for future attacks and can cause future legal issues. Plus, paying a ransom is never a guarantee that attackers will return the victim's data -- or that they won't use it in extortion attacks in the future.

Read more on whether to make ransom payments.

Ransomware negotiation services can sometimes help reduce ransom payment amounts, for victims that choose that path. These specialized third-party brokers act as intermediaries between attackers and victims. They are better equipped to handle negotiations because they are well versed in ransomware groups and their demands.

Read more about ransomware negotiation services and what to expect from them.

The total cost of a ransomware attack, however, far exceeds the ransom price tag. IBM's "Cost of a Data Breach Report 2023" found the average dollar amount attached to a ransomware attack was $5.13 million, an increase of 13% over the previous year—and that doesn't even include the cost of the ransom payment.

The difference can be attributed to multiple factors, including the following:

- Data exposure or loss.
- System downtime.
- Lost productivity.
- Revenue loss.
- Legal and regulatory compliance fines.

Ransomware can also have the following affects:

- Damaged business reputation.
- Lowered employee morale.
- Loss of customer trust and loyalty.
- Organization becomes a potential target for future attacks.

Cyber insurance could help lessen the financial burden of a ransomware attack. Cyber insurance services generally offer pre-breach services -- such as training, vulnerability scanning and tabletop exercises -- as well as post-breach services, including data recovery efforts and breach investigation assistance. Some cyber insurance services will also work with negotiation services to try to lower ransom payment amounts.

Finding cyber insurance coverage isn't always easy, however. The onslaught of ransomware attacks over the past five years have led to huge losses for cyber insurers, resulting in premium hikes or even denial of coverage for customers.

In this guide:

Research has shown that reporting a breach to law enforcement could lessen the cost of a ransomware incident. IBM's survey found the average cost of a ransomware breach was $5.11 million when law enforcement was not involved, as opposed to $4.64 million when law enforcement was involved.

Decision-makers should discuss whether to report a breach to law enforcement. Security experts and law enforcement recommend any organization affected by ransomware notify the authorities -- such as CISA, the Internet Crime Complaint Center or the organization's local FBI field office. Some organizations are legally required to report ransomware attacks. Public organizations, for example, must report cyberattacks within four business days, per new regulations announced by the Securities and Exchange Commission. In some cases, cyber insurers might not issue payments to victims if they have not notified a federal agency.

Along with deciding whether to report a breach, decision-makers must discuss whether to disclose the attack to the public. No national ransomware attack notification law exists for private companies, but if attacks involve personally identifiable information, organizations must notify the individuals affected.

In this guide:

COMMON RANSOMWARE TARGETS

While certain industries, such as critical infrastructure, education and healthcare, tend to make the headlines when they become ransomware victims, it is important to note that no organization -- regardless of size or industry -- is immune to ransomware attacks.

That said, the Sophos report listed the following as the top 13 ransomware targets by sector:

1. Education.
2. Construction and property.
3. Central and federal government.
4. Media, entertainment and leisure.
5. Local and state government.
6. Retail.
7. Energy and utilities infrastructure.
8. Distribution and transport.
9. Financial services.
10. Business, professional and legal services.
11. Healthcare.
12. Manufacturing and production.
13. IT, technology and telecom.

In this guide:

HISTORY OF RANSOMWARE AND FAMOUS RANSOMWARE ATTACKS

Ransomware has bedeviled organizations and individuals for more than three decades, with the first known ransomware campaign reaching its victims via snail mail in 1989. Harvard-educated biologist Joseph L. Popp, now regarded as the "father of ransomware," sent infected floppy disks to 20,000 people who had recently attended a World Health Organization AIDS conference.

Popp's malware became known as the AIDs Trojan. Upon insertion into a victim's computer, the disk -- which appeared to contain a medical research questionnaire but actually harbored malicious code -- encrypted the system and instructed the victim to mail $189 to a P.O. box in Panama. IT experts soon found a decryption key, but the incident marked the beginning of a new cybercriminal era.

Despite Popp's early efforts, ransomware wouldn't come to mainstream prominence until the 2000s, when internet use soared. Early variants, such as GPCode and Archievus, eventually gave way to more sophisticated strains. Several new types of ransomware and ransomware delivery models emerged in the early 2010s, including locker ransomware, such as WinLock in 2011; RaaS, such as Reveton in 2012; and crypto ransomware, such as CryptoLocker in 2013.

The birth of cryptocurrency in 2009 marked another pivotal moment in the history of ransomware, as it gave threat actors an easy and anonymous way to collect

In this guide:

payments. In 2012, Reveton became one of the first ransomware campaigns in which the attackers demanded victims pay ransoms in bitcoin.

WANNACRY UPS THE ANTE

In 2017, hundreds of thousands of computers running Microsoft Windows fell victim to a new ransomware variant, the notorious WannaCry cryptoworm, in one of the biggest ransomware attacks of all time. The threat actors targeted organizations across 150 countries, including major banks, law enforcement agencies, healthcare organizations and telecommunications firms. WannaCry arguably marked the beginning of a new chapter in ransomware, in which attacks became larger, more lucrative, more destructive and more widespread.

As a worm, WannaCry is able to self-replicate, moving laterally to automatically infect other devices on a network without human assistance. The malware uses the EternalBlue exploit, originally developed by the National Security Agency and leaked by Shadow Brokers hackers, which takes advantage of a vulnerability in Microsoft's implementation of the SMB protocol. Although Microsoft released a software update fixing the vulnerability before the attacks, unpatched systems continue to fall prey to WannaCry infections to this day.

Shortly after the WannaCry attacks began, NotPetya -- a variant of Petya ransomware, which had emerged a year earlier -- started making headlines. Like WannaCry, NotPetya takes advantage of the EternalBue exploit. As wiperware,

In this guide:

however, it destroys victims' files after encrypting them—even if they meet ransom demands.

NotPetya caused an estimated $10 billion in losses worldwide. One of the highest-profile targets, Danish shipping and logistics giant A.P. Moller-Maersk, lost around $300 million in the incident. The CIA has attributed the ransomware attack to a Russian military espionage agency, and according to cybersecurity vendor ESET, around 80% of NotPetya's targets were in Ukraine.

In 2018, another notorious ransomware variant, Ryuk, became one of the first to encrypt network drives and resources and disable Windows System Restore. Ryuk made it virtually impossible for victims to recover their data if they didn't have rollback tools or offline backups already in place, unless they paid the ransoms.

RECENT RANSOMWARE TRENDS

So-called *big game hunting*, in which ransomware operators target large organizations with deep pockets, has exploded in recent years. High-profile ransomware victims and high-impact ransomware attacks have included Colonial Pipeline, JBS USA, the government of Costa Rica, Ireland's national health service, Travelex, CNA Financial and many more.

In this guide:

Most famous ransomware attacks of all time

▼ Colonial Pipeline

The pipeline system owner paid **DarkSide** attackers a $4.4 million ransom payment in May 2021, $2.3 million of which was recovered by the U.S. Justice Department.

Costa Rica

The **Conti** ransomware gang conducted a months-long attack against the Costa Rican government starting April 2022, leading the president to declare a state of emergency.

Impresa

In January 2022, the **Lapsus$** ransomware group attacked Portugal's largest media company, taking down its websites, newspaper and TV channels.

JBS USA

The beef manufacturer paid an $11 million ransom to the **REvil** ransomware group after an attack forced it to shut down operations in May 2021.

Kronos

The workforce management software company's private cloud was hit with ransomware in December 2021, affecting Kronos and its clients.

▲ Maersk

Part of the global **NotPetya** attack in June 2017, Maersk was locked out of its systems worldwide, costing the Danish shipping company a reported $300 million.

▼ Swissport

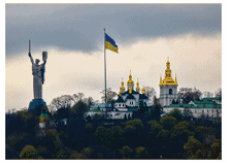
In February 2022, the airport ground and cargo handling services company was hit with a double extortion ransomware attack by the **BlackCat** ransomware group.

▼ Travelex

The foreign exchange company paid $2.3 million out of a demanded $6 million ransom to the **REvil** ransomware group in December 2019.

UK National Health Service

The **WannaCry** ransomware attack hit the U.K.'s NHS in May 2017, affecting medical facilities and services across England and Scotland and costing a reported $100 million.

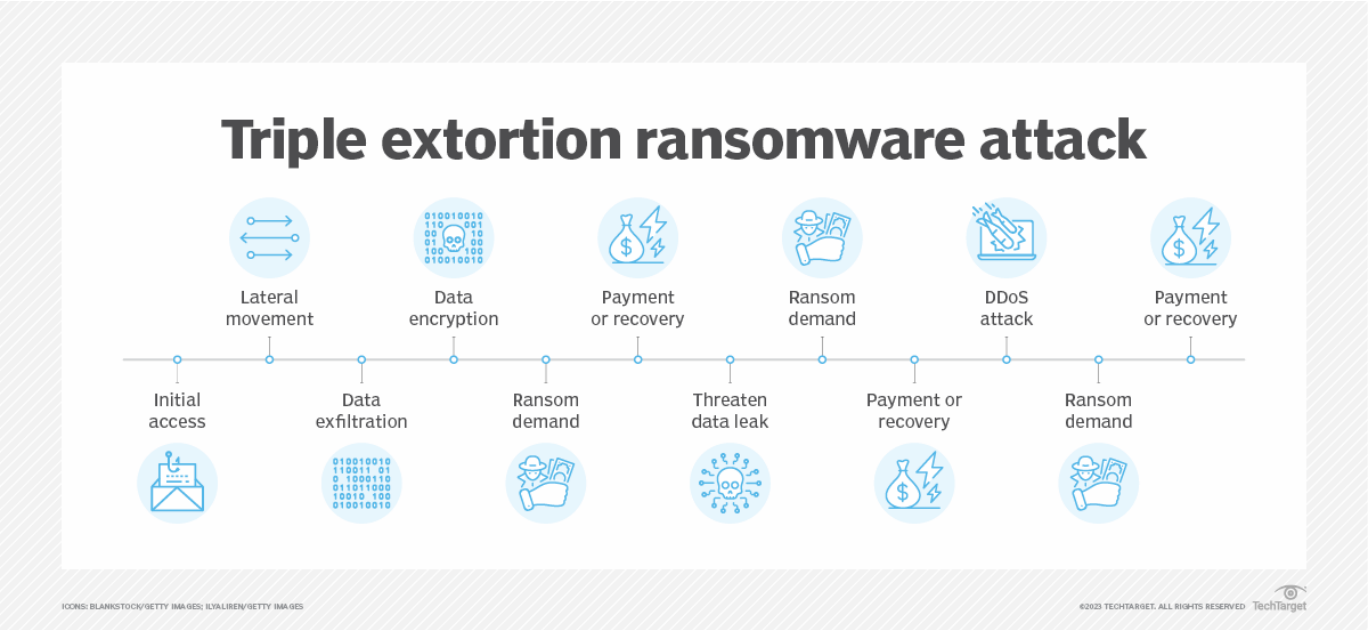


▲ Ukraine

In June 2017, about 80% of the global **NotPetya** attacks targeted government systems, utilities and private organizations in Ukraine.

In this guide:

The late 2010s also saw the rise of new forms of ransomware, including double extortion and triple extortion ransomware. RaaS also continues to grow in popularity and sophistication, making it possible for threat actors with limited technical abilities and resources to become ransomware operators. In 2021, for example, ransomware attributed to the REvil gang's RaaS operation hit managed service provider Kaseya, in one of the largest ransomware episodes ever. More than 1 million devices became infected.



In this guide:

HOW TO PREVENT RANSOMWARE ATTACKS

Ransomware prevention is a huge challenge for organizations of all types and sizes, with no magic-bullet remedy. Experts say enterprises need a multi-pronged ransomware prevention strategy that includes the following:

- **Defense-in-depth security.** A defense-in-depth approach has layered security controls that work in concert to block malicious activity. If malware manages to sneak past one control, the hope is that another overlapping security mechanism will stop it.

  Experts recommend, at a minimum, deploying foundational cybersecurity tools and strategies such as antimalware, multifactor authentication, firewalls, email security filtering, web filtering, network traffic analysis, allowlisting/denylisting, endpoint detection and response, the principle of least privilege and secure remote access technologies, including VPNs and zero-trust network access. They also advise organizations to limit or block the use of RDP.

- **Advanced security controls.** While basic cybersecurity controls can recognize and catch many known ransomware variants, advanced protection technologies are more likely to uncover novel attacks. Consider tools and strategies such as extended detection and response (XDR), managed detection and response, Secure Access Service Edge, SIEM, user and entity behavior analytics, zero-trust security and cyber deception.

- **Patch management.** When the WannaCry ransomware attack first struck in May 2017, it took advantage of a known vulnerability for which Microsoft had

released a patch two months earlier -- one that hundreds of thousands of victims had not yet deployed. Remarkably, organizations with unpatched systems still continue to fall victim to WannaCry and many other legacy attacks.

While organizations sometimes have good reasons for delaying software and system updates -- because patches can cause performance issues that affect business operations, for example -- they must weigh them against the costs of potentially catastrophic security incidents. Follow patch management best practices to dramatically reduce the risk of ransomware.

- **Data backups.** Backups of critical data can effectively short-circuit a ransomware attack, letting an organization restore operations without entertaining cybercriminals' demands. Crucially, however, the backup must be inaccessible from the primary IT environment so threat actors can't find and encrypt it during the intrusion. It is also important to note that while backups are an important part of ransomware defense, they are not a cure-all, especially in the event of double or triple extortion attacks.

  Organizations that use cloud-based backups for ransomware protection must know the right questions to ask providers to ensure their data is in good hands.

- **Security awareness training.** Ransomware operators frequently gain access to corporate networks via detectable and preventable means. End-user education is arguably the most important -- and the most difficult -- element of malware prevention. Security awareness training should be dynamic and engaging, and it should include specifics about ransomware to teach users both how to avoid attacks and what to do if they think one might be underway.

In this guide:

HOW TO DETECT ATTACKS

Even organizations that follow ransomware prevention best practices will inevitably fall victim to attacks. In fact, many experts say companies should consider it not a question of if but when.

If security teams can detect a ransomware attack in its early stages, however, they might be able to isolate and remove malicious actors before they have time to find, encrypt and exfiltrate sensitive data.

An important first line of defense is antimalware tools that can recognize known ransomware variants based on their digital signatures. Some offerings, such as XDR and SIEM platforms, also scan for behavioral anomalies to catch novel and otherwise unrecognizable ransomware strains. Possible indicators of compromise include abnormal file executions, network traffic and API calls -- any of which could point to an active ransomware attack.

Some organizations use deception-based detection to flush out adversaries, baiting them with fake IT assets that act as tripwires to alert security teams to their presence. While cyber decoys require considerable resources to deploy and maintain, they have exceptionally low false-positive rates, making them valuable weapons in the fight against ransomware.

In this guide:

In this guide:

HOW TO REMOVE RANSOMWARE

Any credible suggestion that a ransomware intrusion is underway should automatically trigger the first step of a ransomware incident response plan: validation of the attack. If the security team confirms the incident is indeed a ransomware attack, it can then proceed to the following steps:

- **Gather the incident response team.** This group should include representatives from IT, executive management, legal and PR teams. Crucially, everyone should know the following well in advance of an actual crisis:
  - How they will receive notification of an incident.
  - Their particular roles and responsibilities.
  - How to communicate with each other.
- **Analyze the incident.** Work as quickly as possible to determine how far the malware has spread.
- **Contain the incident.** Immediately disconnect and quarantine any infected systems and devices in an effort to minimize the malware's impact. Ideally, network management technology is in place that can automatically quarantine endpoints displaying atypical behavior, block C&C server connections and lock down network segments to prevent lateral movement. Automation can dramatically expedite the containment process when time is of the essence. After containing the infection, check backup resources to confirm they are intact and secure.

In this guide:

- **Investigate.** Gather as much information as possible about the ransomware attack and its severity. Assess potential outcomes and make recommendations to executive decision-makers.
- **Eradicate malware and recover from the incident.** Delete and replace infected central system instances, and wipe and restore affected endpoints with clean backup data. Next, scan the restored data to confirm the malware is gone. Finally, change all system, network and account passwords.
- **Contact stakeholders.** Communicate the specifics of the incident to appropriate stakeholders, as the incident response plan dictates. These might include internal stakeholders, such as employees and executive leadership, and external stakeholders, such as customers, third-party partners and law enforcement.
- **Conduct post-incident activities.** Disclose attacks to government organizations and customers as necessary, in keeping with compliance regulations and company policies. Confirm all systems, data and applications are accessible and operational, with no outstanding vulnerabilities that could let attackers back into the environment.
- **Perform analysis and learn from the attack.** Once the dust has settled and the organization is again operating normally, carefully analyze the details of the attack and identify any security gaps the organization needs to address to prevent future episodes. Review incident response efforts, identify lessons learned and update the incident response plan accordingly.

In this guide:

Make sure postmortem analysis doesn't involve pointing fingers or assigning blame. Rather, highlight the opportunity to learn from any missteps and make future ransomware prevention and response efforts stronger.

Read more about how to recover from a ransomware attack.

Sharon Shea is executive editor of TechTarget Security.

Alissa Irei is senior site editor of TechTarget Security.

CONTINUED READING

The biggest ransomware attacks in history

How to recover from a ransomware attack

How to prevent ransomware, step by step