

Ransomware Groups Explained: How They Operate, Who They Target, and How to Defend Against Them

Ransomware has grown from a nuisance spread by opportunistic hackers into a professional criminal industry that disrupts hospitals, fuel pipelines, schools, and city governments. At the centre of this industry sits every [ransomware group](#), a team of cybercriminals that breaks into networks, steals data, locks files, and demands payment. Chainalysis reported that victims paid more than one billion US dollars in ransom during 2023, which shows how profitable this business has become. Understanding how these crews think is therefore the first step toward protecting data, money, and public trust.



Think of a school exam where students try to guess what the teacher will ask. In the same way, defenders who know the usual questions an attacker asks, such as which password is weak or which server is unpatched, can prepare answers in advance. This article explains how ransomware gangs are structured, how a typical attack unfolds, which real incidents teach the best lessons, and what practical defences work. It also shows how digital risk protection helps security teams spot trouble before encryption begins.

What Is a Ransomware Group?

A ransomware group is an organised set of cybercriminals that develops or rents malicious software to encrypt a victim's files and demand money for the decryption key. Many such groups also steal sensitive data first and threaten to publish it on a leak site if the victim refuses to pay. Security researchers often call them ransomware threat actors, a term that covers developers, affiliates, access sellers, and negotiators. In short, they run a business, complete with brand names, support chats, and revenue targets.

Law enforcement agencies such as the FBI and the UK National Crime Agency track these crews through their malware families, infrastructure, and cryptocurrency wallets. Names change often, because when one brand is exposed, members frequently rebrand or join a competitor. For students, a useful comparison is a franchise restaurant, where the head office supplies the recipe and local owners run each shop. Here the recipe is the malware, and the shops are the affiliates who attack victims.

How Ransomware Gangs Are Organised

Modern ransomware gangs rarely work as one small team typing commands in a basement. They divide labour the way a company does, with developers, recruiters, technical operators, and negotiators who behave like a customer-service desk. This specialisation makes attacks faster, easier to scale, and harder to trace back to a single person. Knowing each role helps defenders see where the attack chain can be broken.

The Ransomware-as-a-Service Model

In the [ransomware-as-a-service](#) model, developers build the malware and the leak site, then lease them to affiliates who carry out the break-ins. The developers keep a share of each ransom, and the affiliates keep the rest. This arrangement lets technically modest criminals launch serious attacks, which is why incidents keep rising even when one brand disappears.

Initial Access Brokers

Initial access brokers are specialists who sell stolen remote-desktop logins, VPN credentials, or footholds inside corporate networks. Their customers are affiliates who prefer to skip the break-in step and move straight to data theft and encryption. Because these sales happen on underground forums, monitoring them can give defenders early warning that their company is on the market.

Negotiators and Support Teams

Many crews employ negotiators who chat with victims through a Tor-based portal and push for payment using deadlines and discounts. Some even offer "support" for decryption problems,

which sounds absurd but reflects their business mindset. Recognising these pressure tactics helps incident response teams stay calm and avoid rushed decisions.

How a Ransomware Attack Unfolds Step by Step

A typical intrusion follows a predictable path, which is good news because predictable paths can be interrupted. Frameworks such as MITRE ATT&CK document these behaviours in detail and give defenders a shared vocabulary. Attackers may spend days or weeks inside a network before anyone notices anything unusual. The visible encryption event is usually the final step, not the first.

Initial Access

Attackers gain entry through phishing emails, exposed remote services, stolen passwords, or unpatched software vulnerabilities. Weak or reused credentials without multi-factor authentication remain among the most common doors left open. Closing these doors costs far less than recovering from a full breach.

Lateral Movement and Data Theft

Once inside, intruders explore the network, escalate privileges, and locate backups and valuable files. They then copy sensitive information to servers they control, a step known as data exfiltration that prepares the ground for double extortion. The Maze crew is widely credited with popularising this tactic in late 2019.

Encryption and Extortion

Finally, the attackers delete or encrypt backups, launch the encryption tool across many machines, and drop a ransom note. The note explains how to contact the criminals and warns that stolen data will be published if payment is delayed. At this point, the victim faces an operational outage and a privacy crisis at the same time.

Real-Life Examples of Ransomware Attacks

Real cases teach better than theory, so let us look at three incidents that made global headlines. Each one shows a different weakness, from a single missing security control to a supply chain flaw. Reading them carefully helps students see that attacks succeed through ordinary mistakes more often than through movie-style hacking. The details below come from US government statements, court filings, and testimony given to lawmakers.

Colonial Pipeline (2021)

In May 2021, the DarkSide crew attacked Colonial Pipeline, and the company halted operations as a precaution, which caused fuel shortages across parts of the US East Coast. The company

paid roughly 75 bitcoin, about 4.4 million US dollars, and the US Department of Justice later recovered a portion of it. According to testimony given to US lawmakers, the intrusion began with a compromised VPN account that lacked multi-factor authentication.



Kaseya (2021)

In July 2021, affiliates of REvil exploited a vulnerability in Kaseya's VSA remote-management software and pushed ransomware through managed service providers to their customers. Estimates suggested that roughly 1,500 downstream businesses were affected, even though only a small number were direct Kaseya customers. This case shows why supply chain risk deserves the same attention as internal security.

Change Healthcare (2024)

In February 2024, the ALPHV crew, also known as BlackCat, attacked Change Healthcare and disrupted insurance claims and pharmacy services across the United States. UnitedHealth Group's chief executive told lawmakers that the company paid a 22 million dollar ransom and that attackers used stolen credentials on a portal without multi-factor authentication. The episode proved that one weak entry point can ripple through an entire national healthcare system.

Law Enforcement Pressure and the Cycle of Rebranding

Governments have become more aggressive against [ransomware gangs](#), using arrests, sanctions, indictments, and infrastructure takedowns. In February 2024, the UK National Crime Agency and the FBI, working with international partners, disrupted LockBit's infrastructure in an effort known as Operation Cronos. Such actions damage trust among affiliates, because members fear that their identities or wallets may be exposed. However, the criminal market adapts quickly, and some brands return in weaker form or are replaced by new ones.

The Conti brand offers another lesson. After leaked internal chats and a high-profile attack on Costa Rica in 2022 drew intense attention, the brand wound down and its members reportedly spread into smaller crews. This pattern means defenders should track behaviours and techniques rather than rely only on group names. It is like recognising a thief by the way they pick a lock instead of by the jacket they wear.

Warning Signs That Attackers May Already Be Inside

Early detection can turn a catastrophe into a minor incident. Security teams that watch for subtle behaviour changes often catch intruders before encryption starts. The signals below deserve immediate investigation, especially when several appear together. Treat them as a starting checklist for your monitoring and incident response playbooks.

- Logins from unusual locations or at odd hours, especially on administrator accounts
- New privileged accounts or sudden permission changes that nobody requested
- Security tools, logging, or backup services switched off without approval
- Large outbound data transfers to unfamiliar destinations
- Remote-access tools or scripting utilities appearing on servers where they do not belong
- Company credentials offered for sale or discussed on underground forums

Digital Risk Protection: Seeing the Threat Before It Strikes

[Digital risk protection](#) is a security discipline that monitors the open web, deep web, and dark web for threats aimed at an organisation's brand, people, and data. For ransomware defence, it can reveal leaked employee credentials, mentions of the company on criminal forums, and fake domains used for phishing. This outside-in view complements internal tools such as endpoint detection and firewalls, which only see what happens inside the network. Together, they give security teams a fuller picture of their attack surface.

Consider a simple example in which a staff member reuses a work password on a personal website that later suffers a breach. A good monitoring service can flag that exposed password, letting the organisation reset it before an access broker sells it. Alerts about a post on a leak site can also help legal and communications teams respond quickly. These capabilities connect naturally with threat intelligence, attack surface management, and takedown services.

Dark Web Monitoring

Dark web monitoring watches criminal marketplaces, paste sites, and forums for stolen credentials, internal documents, and chatter about your company. When a match appears, analysts verify it and alert the security team. Acting within hours rather than weeks can decide whether stolen access is ever used.

Brand and Domain Protection

Attackers often register look-alike domains to trick employees or customers into entering passwords. Brand protection tools detect these domains and support takedown requests with registrars and hosting providers. Removing a phishing site early reduces the chance that someone clicks and hands over a login.

A Practical Defence Checklist

No single product stops every attack, so strong defence relies on layers that cover people, process, and technology. Government guidance such as the CISA #StopRansomware Guide and the NIST Cybersecurity Framework 2.0 recommends similar foundations. The goal is to make intrusion harder, limit how far attackers can move, and ensure fast recovery. Use the list below as a practical starting point for your own organisation.

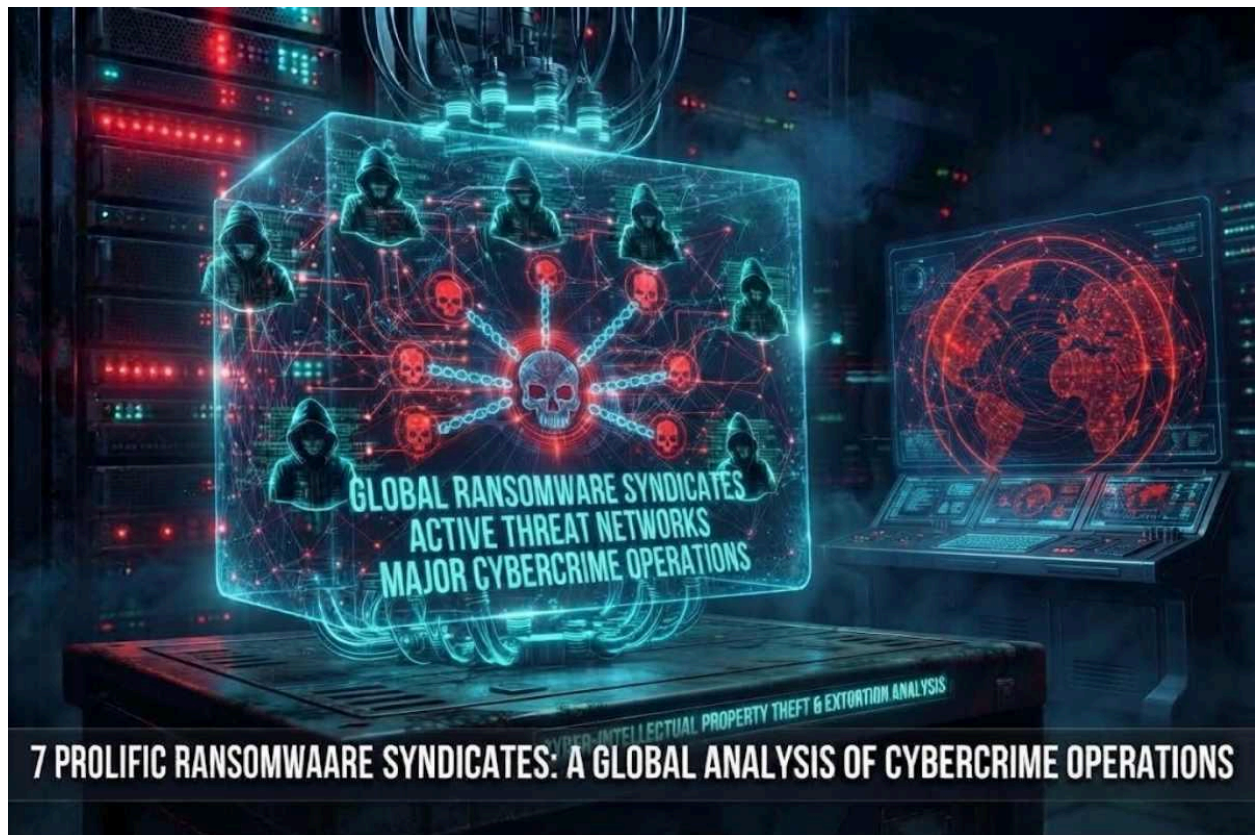
- Enforce multi-factor authentication on email, VPN, remote access, and all administrator accounts
- Patch internet-facing systems quickly, prioritising vulnerabilities known to be exploited
- Keep offline or immutable backups following the 3-2-1 rule, and test restores regularly
- Segment networks and apply least-privilege access so one stolen account cannot open everything
- Deploy endpoint detection and response with round-the-clock monitoring
- Train staff to recognise phishing and report suspicious messages without fear of blame
- Write and rehearse an incident response plan that includes legal, communications, and leadership roles

Common Mistakes Organisations Make

Even well-funded organisations repeat the same errors, and most are about process rather than technology. Attackers study these habits and build their playbooks around them. Learning from other people's mistakes is the cheapest form of security training. Three errors appear again and again in public incident reports.

Trusting Backups Without Testing Them

Many companies discover during a crisis that their backups are incomplete, outdated, or reachable from the same network the attackers control. A backup that has never been restored is only a hopeful assumption. Regular restore drills turn that assumption into evidence.



Ignoring Third-Party Risk

Vendors, software suppliers, and managed service providers often hold privileged access to your systems. The Kaseya case showed how one supplier weakness can spread to thousands of organisations. Reviewing vendor security and limiting their access reduces this hidden exposure.

Deciding About Payment Under Pressure

Agencies such as the FBI and CISA discourage paying, because payment does not guarantee data recovery and may encourage further attacks. Paying can also carry legal risk if the recipient is under sanctions. Organisations should decide their position, consult legal counsel, and involve law enforcement before a crisis, not during one.

Conclusion: Knowledge Is the Strongest Defence

Every ransomware group depends on ordinary weaknesses such as missing multi-factor authentication, unpatched software, reused passwords, and untested backups. Cases like Colonial Pipeline, Kaseya, and Change Healthcare show how these gaps become headline events. The criminals are organised, but their methods follow patterns that defenders can learn, detect, and disrupt. Preparation, speed, and visibility consistently beat panic.

Frequently Asked Questions (FAQ)

What does ransomware actually do to a computer?

It encrypts files so they cannot be opened, then displays a message demanding payment for the key. Many variants also copy data before locking it, so the victim faces a leak threat as well.

How do attackers usually get into a network?

The most common routes are phishing emails, stolen or reused passwords, exposed remote-access services, and unpatched software. Multi-factor authentication and prompt updates close many of these doors.

What is double extortion?

Double extortion means attackers both encrypt files and threaten to publish stolen data. Even a victim with perfect backups can still be pressured because the leak threat remains.

Should a victim pay the ransom?

Government agencies advise against it, because payment does not guarantee recovery and can fund future crime. The decision involves legal, financial, and ethical factors, so consult experts and law enforcement first.

Can small businesses be targeted?

Yes, because smaller firms often have fewer security controls and are seen as easier victims. Attackers also use automated scanning, so size does not protect you from being found.

What should I do first if I suspect an infection?

Isolate affected devices from the network, but do not wipe them, since evidence is valuable. Then contact your incident response team or a trusted specialist and notify the relevant authorities.