45 Ransomware Statistics Vital for Security in 2026

By Panda Security

Published: 2026-01-26 · Archived: 2026-04-05 14:45:25 UTC

Ransomware is a type of cyberattack where criminals lock your files and demand money to unlock them. Your photos, documents or work files suddenly become unusable. A message pops up asking for payment, often with a deadline and a threat to delete everything if you don't pay.

These attacks don't just hit big companies. Home users get caught, too. In fact, the United States is the most targeted country for ransomware attacks, with millions of people and businesses affected every year.

Check out 45 ransomware statistics that show who's being targeted, how attacks are spreading and how expensive the damage can be. We'll also share some tips on how to detect ransomware — and ways to avoid it.

Key Ransomware Trends in 2026

Ransomware keeps changing fast. Modern hackers aren't just locking your files anymore. They steal it, pressure you online and use smarter tricks to break in. Here are some key ransomware trends to help you spot where the threat is heading and why you should care.

Double Extortion and Data Exfiltration

Attackers now steal your data before they lock it. Once they have that sensitive info, they threaten to publish it online if you don't pay up. Some cybersecurity reports show that data theft is part of about 74% of ransomware incidents, outpacing old-school "just encryption" tactics.

Because of this, backups alone aren't enough. Even if you recover files, the threat of leaked personal or financial info still hangs over you.

AI-Enhanced Phishing and Social Engineering

Cyber criminals are using AI tools to create highly convincing scam messages. These emails and texts sound natural, look professional and often feel personal. Many are written to mimic trusted companies, coworkers or even friends.

Because these scams are harder to spot, more people are being tricked into clicking on malicious links or sharing login details. That first mistake often opens the door to a ransomware attack.

The Expansion of Ransomware as a Service (RaaS)

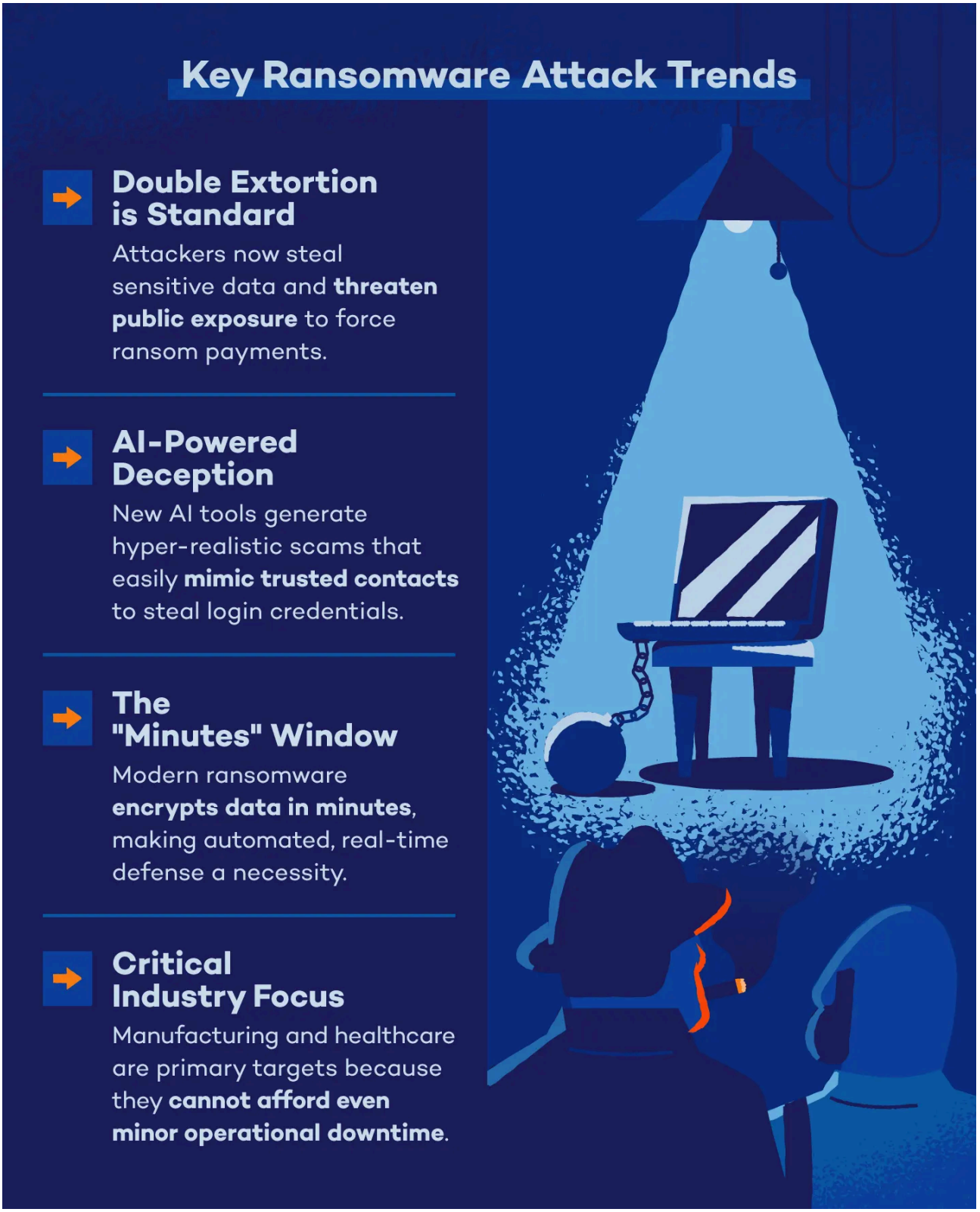
RaaS has lowered the barrier to entry for cybercriminals. Instead of building malware from scratch, attackers can now subscribe to ready-made ransomware kits and support tools. Even inexperienced threat actors can launch full-scale attacks with minimal effort.

This service model has led to a steady rise in active ransomware groups and a larger pool of affiliates. More players in the game means more frequent attacks, faster shifts in tactics and a noisier threat landscape overall.

Faster Encryption Speeds

Modern ransomware can lock up data in minutes, leaving little time to stop it. While exact times vary by strain and system size, analysts note that fast encryption has become a core part of attack tactics to outpace human response and security tools.

That means the window to detect and block a breach is shrinking. Quick reaction and automated defenses are no longer optional.



How Common Is Ransomware?

Ransomware isn't rare. It's constant and noisy, and far more common than most people realize. And the numbers make that clear very quickly.

Here's a snapshot of how widespread ransomware attacks really are:

1. Over **1.3 million** ransomware attacks targeted the U.S. in 2024. (Statista)

2. Right behind the U.S., Thailand recorded about **1.1 million** ransomware detections in 2024. (Statista)

3. Worldwide ransomware detections peaked at **632 attempts** in November 2024 alone. (Statista)

4. **100%** of organizations that had data encrypted reported direct human impact. Every ransomware incident affected real people behind the screens. (Sophos)

5. **41%** of IT and security teams reported increased anxiety after an attack. And that stress doesn't stay at work. (Sophos)

6. **34%** of teams felt guilty for not stopping the attack in time. For home users, that same delay can mean not noticing an infection until files are already locked. (Sophos)

7. **31%** of teams experienced staff absence due to stress or mental health issues related to the attack. (Sophos)

8. Remote access compromise was the most common attack vector in early 2025, causing nearly **40%** of the cases. (Coveware)

9. Phishing followed remote access compromise, causing nearly **30%** of the cases. (Coveware)

10. The top six ransomware variants are Akira, Qilin, Lone Wolf, Silent Ransom, Shiny Hunters and DragonForce. They made up over **50%** of attacks in Q2 2025. (Coveware)

11. Akira and RansomHub held a combined **25%** market share in late 2024. (Statista)

12. Clop ransomware was the **most discussed strain** on dark web forums in 2024. (Statista)

13. In **a quarter** of ransomware cases, leadership was replaced after the attack. (Sophos)

Ransomware Cost and Payment Statistics

Ransomware is big money. Attackers continue to demand eye-watering sums, even as more victims push back or refuse to pay.

Here's a clear look at the latest ransomware cost and payment statistics:

14. **32%** of ransomware attacks worldwide resulted in a ransom payment in Q3 2024 — down from 36% in the previous quarter. (Statista)

15. Global ransomware revenue fell from **$1.2 billion** in 2023 to about **$814 million** in 2024. (Statista)

16. The average ransom payment in 2024 in the United States reached nearly **$490,000**. (Statista)

17. The median ransom demand in 2025 was over **$1.3 million**. (Sophos)

18. That median demand dropped by **34%** compared to 2024, when it was **$2 million**. (Sophos)

19. The median ransom payment fell **50%**, from **$2 million** in 2024 to **$1 million** in 2025. (Sophos)

20. Large payments of **$5 million** or more dropped from **31%** of cases in 2024 to **20%** in 2025. (Sophos)

21. **53%** of victims negotiated and paid less than the original ransom demand. (Sophos)

22. Only **29%** of victims paid exactly what attackers initially demanded. (Sophos)

23. **18%** of victims ended up paying more than the initial demand. (Sophos)

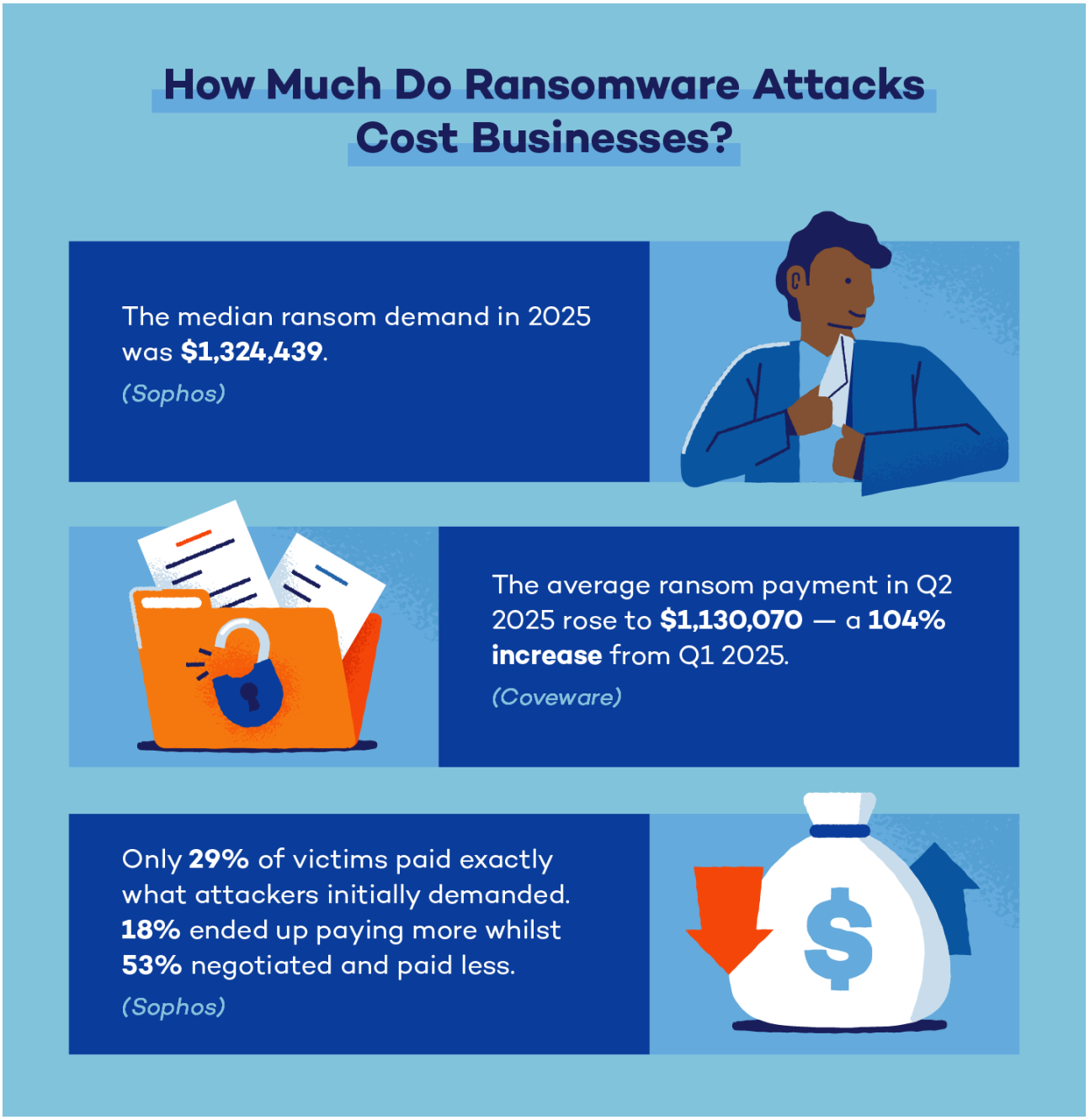
24. The average ransom payment in Q2 2025 rose to **$1.1 million** — a **104%** increase from Q1 2025. (Coveware)

25. The median ransom payment in Q2 2025 reached **$400,000**, up **100%** quarter over quarter. (Coveware)

26. Only **26%** of organizations chose to pay a ransom, a rate that remained stable throughout 2025. (Coveware)

Ransomware doesn't just cost victims money after an attack. It's also driving massive spending on prevention.

The global ransomware protection market was valued at about $32.6 billion in 2024 and is expected to reach nearly $123 billion by 2034, growing at around 14% per year. This investment reflects how expensive and disruptive ransomware has become, even when no ransom is paid.



Ransomware attacks continue to surge worldwide, hitting countries at very different scales. Some regions face occasional waves, while others deal with nonstop targeting year-round. The U.S. and Thailand take the first two spots, respectively, among the top 10 countries targeted by ransomware.

Here are the remaining eight countries (Statista):

Country	Ransomware detections in 2024
1. Turkey	514K
2. Taiwan	474K
3. Japan	394K

Country	Ransomware detections in 2024
4. Brazil	242K
5. Germany	240K
6. India	209K
7. South Korea	182K
8. Singapore	169K

Top Ransomware Groups to Watch

Both long-running and newer ransomware groups continue to cause serious damage worldwide. Recent reporting shows a busy and fragmented threat landscape, with a small number of groups driving a large share of activity — and many attacks still going unattributed.

Here are some key ransomware statistics about threat groups:

27. **78** ransomware incidents were publicly disclosed in December 2025 alone. (BlackFog)

28. **25** different ransomware groups claimed victims in December 2025. (BlackFog)

29. Health care was the most targeted industry, with **14** attacks. (BlackFog)

30. The United States accounted for **46%** of all reported incidents. (BlackFog)

31. Australia followed at **14%**, showing a sharp drop after the top target. (BlackFog)

Based on recent activity and visibility, ransomware groups Akira, Everest, INC, LockBit and Clop stand out as top threats to watch for.

Most Common Tactics, Techniques and Procedures

Ransomware attacks follow patterns. By tracking how threat actors operate, you can spot attacks earlier and reduce damage.

Here are the most common malware tactics used in early 2025:

32. **74%** of ransomware cases involved data exfiltration, which is now the main pressure tactic. (Coveware)

33. **60%** of cases showed lateral movement across networks. Attackers move between systems to expand access and maximize impact. (Coveware)

34. **47%** of cases involved confirmed impact activity. This includes file encryption and operational disruption. (Coveware)

35. **90%** of impacted cases still involved encryption. Even as tactics evolve, encryption remains a core method. (Coveware)

36. **47%** of incidents involved defense evasion techniques. Attackers work to stay hidden long enough to finish the attack. (Coveware)

37. **42%** of ransomware cases involved discovery activity. Attackers map networks and identify high-value systems before striking. (Coveware)

Ransomware Statistics by Industry

Ransomware doesn't hit all industries equally. Attackers tend to focus on sectors where disruption causes immediate pressure to pay and where sensitive data carries real value. Recent ransomware statistics make those patterns clear.

Here's how ransomware activity breaks down by industry:

38. **Professional services** accounted for **19.7%** of ransomware attacks in Q2 2025. This includes legal, consulting and business services where downtime quickly becomes costly. (Coveware)

39. **Consumer services** made up **13.7%** of attacks since customer-facing businesses are attractive targets due to payment data and operational pressure. (Coveware)

40. **Health care** also represented **13.7%** of ransomware incidents. Health care remains a prime target because disruptions can affect patient care. (Coveware)

41. The **public sector** accounted for **9.4%** of ransomware attacks. Government and public services remain exposed due to legacy systems and wide user access. (Coveware)

42. Financial services represented **7.7%** of ransomware activity. Attackers target both money and large volumes of sensitive customer data. (Coveware)

43. Financial institutions recorded **3,336 cyber incidents** worldwide in 2024. Ransomware plays a major role in these incidents. (Statista)

44. **927** of those financial sector incidents resulted in sensitive data leakage. This shows how often ransomware goes beyond file encryption. (Statista)

45. **Real estate** and **utilities** each accounted for just **0.9%** of ransomware attacks. Lower digital exposure and stronger controls may reduce their appeal to attackers. (Coveware)

How to Prevent a Ransomware Attack

To understand prevention, it helps to know what ransomware does. It sneaks in quietly, blocks access to your files and pressures you to pay to get them back. Most attacks rely on everyday mistakes, and you can avoid them easily.

Here are some ways to reduce the risk and prevent ransomware:

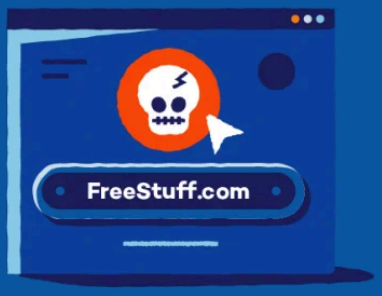
- **Keep your devices updated:** Updates fix known security holes. Skipping them leaves doors open for ransomware and other malware.
- **Use a strong password manager:** Weak or reused passwords are a common entry point. Our password statistics show that 1 in 4 people have at least one account compromised due to weak passwords. A password manager creates and stores strong, unique passwords so you don't have to.
- **Be cautious with links and attachments:** Ransomware often starts with a click. If a message feels rushed, unexpected or off, don't open it.
- **Back up your files regularly:** Save copies of important files to an external drive or secure cloud storage. If ransomware strikes, backups give you a way out without paying.
- **Install trusted security software:** A reliable anti-ransomware solution can block malicious files, warn you about risky sites and help you get rid of malware if something slips through.
- **Remove apps you don't use:** Old or unused software can become an easy target. Less clutter means fewer weak spots.

For organizations, ransomware prevention involves more layers: employee training, endpoint protection, access controls and tested recovery plans. But it's still people who feel the impact when systems go down, data is lost or stress spikes after an attack.

How to Prevent Ransomware Attacks

Back up your files regularly

Save copies of important files to an external drive or secure cloud storage so if ransomware strikes, backups give you a way out without paying.



Never open suspicious links or attachments

If a message feels rushed, unexpected or off, don't open it.

Use a strong password manager

Weak or reused passwords put you at risk. Password managers help you create and store strong, unique passwords.

Keep devices updated

Updates fix known security holes. Skipping or postponing them leaves you vulnerable to ransomware and other malware.

Install trusted security software

Protect Your Digital Life With Panda Security

Ransomware statistics make one thing clear: Attacks are getting smarter, faster and harder to spot. Panda Security helps you stay ahead with tools designed for real-world threats, such as Panda Dome Antivirus for real-time protection.

From blocking malicious files to stopping suspicious links before they load, Panda focuses on prevention first. Our tools include features like ransomware defense, web filtering and cloud-based threat detection. They help prevent ransomware and keep your personal data protected across your devices.

Explore Panda Dome's security suite and see how we can help keep your data safe.

Panda Security specializes in the development of endpoint security products and is part of the WatchGuard portfolio of IT security solutions. Initially focused on the development of antivirus software, the company has since expanded its line of business to advanced cyber-security services with technology for preventing cyber-crime.

Source: https://www.pandasecurity.com/mediacenter/malware/locky-ransomware-strikes-amazon/