Navigating Ransomware in 2025:

Key Insights and Prevention Strategies

Digital Security
Progress. Protected.

Ransomware Landscape, Prevention & Beyond

Ransomware remains one of the most pressing cybersecurity threats in 2025, continuing to evolve in both sophistication and impact. Despite years of advancements in cybersecurity, organizations of all sizes and across all industries still face relentless attacks that penetrate their defenses through increasingly refined techniques. One of the latest developments in this ongoing battle is the use of **EDR killers**—malware designed to disable endpoint detection and response (EDR) solutions before deploying ransomware. This demonstrates how threat actors adapt to security advancements to exploit weaknesses in company defense.

The motivation behind ransomware attacks remains high, driven not only by financial incentives but also by tactical and strategic goals. While cybercriminal groups deploy ransomware primarily for profit, APT groups may utilize ransomware to cover tracks or as a destructive tool for disrupting critical infrastructure—often with geopolitical consequences. This evolving use of ransomware adds further complexity to the threat landscape. Both financially motivated ransomware groups and APT actors continuously refine their techniques, leveraging supply chain compromises, zero-day exploits, and AI-assisted phishing to maximize their reach and impact.

$4.91 million

was the average cost of a ransomware attack in 2024.

Source: *IBM: Cost of a Data Breach Report 2024*

In this ever-evolving threat landscape, **prevention** remains the single most effective measure organizations can take to strengthen their security posture. While incident response and recovery are critical, stopping ransomware before it gains a foothold reduces both operational disruption and financial loss.

A preventive security strategy—including robust patch management, zero-trust architecture, AI-native protection, password management policies, multi-factor authentication (MFA), employee awareness, and continuous threat monitoring—can significantly lower the risk of ransomware infiltration.

As we move forward in 2025, the ability to anticipate, prevent, and neutralize ransomware threats before they materialize is more crucial than ever. That includes having powerful **remediation technology** ready to help you 24/7/365.

Latest Observations on Ransomware

Several key ransomware trends from 2024 are set to shape the threat landscape and defense strategies in 2025. Keeping them in focus is essential for staying ahead of evolving risks.

One of the most notable events in 2024 was the dismantling of LockBit, previously the leading ransomware-as-a-service (RaaS) group disseminating the most deployed ransomware variant across the world. The disruption of LockBit has created a significant vacuum in the ransomware landscape. This gap was quickly filled by other ransomware actors, with **RansomHub** emerging as the **most successful so far**.

By the end of H2 2024, RansomHub had listed almost 500 victims, establishing itself as a dominant player in the ransomware ecosystem. Until now, RansomHub has encrypted and exfiltrated data from victims across a wide range of industries: IT, government services and facilities, healthcare, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, or critical infrastructure sectors such as communications.

Although RaaS is a highly competitive cybercriminal environment where gangs continuously innovate and adjust their affiliate programs to attract more partners and increase profitability, ESET expects RansomHub to maintain its dominant position throughout 2025. This is due not only to its **aggressive tactics** and sophisticated methods for maintaining control over compromised networks and exploiting vulnerabilities in systems, but also to its **ability to attract affiliates** formerly associated with LockBit and BlackCat.

As the RaaS model continues to evolve, ransomware threat actors are increasingly adopting specialized techniques to evade detection and increase damage. While Endpoint Detection and Response (EDR) killers have long been used by ransomware groups, their prevalence has grown, with some gangs now developing custom tools and offering them as part of their RaaS programs. At the same time, many ransomware actors entering the

RaaS ecosystem follow trends set by established groups, often coding their encryptors in Rust or Go to ensure cross-platform compatibility and broader reach.

EDR KILLERS are specialized malware designed to disable security solutions by leveraging BYOVD techniques. Attackers first install legitimate but vulnerable drivers and then exploit them to execute privileged actions from kernel space. This allows them to bypass security controls, terminate security processes, and disable detection and protection mechanisms.

As EDR killers have become a common part of ransomware attacks, ESET expects the most advanced actors to improve this type of tooling in 2025, making it increasingly sophisticated, protected, and harder to detect. What this trend shows is that security tools like **EDR are a thorn in the side of cybercriminals** who will try hard to remove them or at least turn them off.

RaaS and advanced techniques should not be discussed without recognizing the involvement and the role of Advanced Persistent Threat (APT) groups. These groups leverage ransomware not only for financial gain but also to achieve broader strategic objectives. The following APT groups have recently become more involved in ransomware attacks:

ChamelGang (China-aligned)

This group has been observed using ransomware to distract from their covert operations, making it harder for defenders to detect their primary activities.

This group, sometimes also going by the name CamoFei, has been using the CatB ransomware strain in attacks that impact high-profile organizations worldwide, including government organizations such as Presidency of Brazil or critical infrastructure such as All India Institute of Medical Sciences (AIIMS), a public medical research university and hospital.

Moonstone Sleet (North Korea-aligned)

Known for developing and deploying their own ransomware FakePenny, Moonstone Sleet uses ransomware primarily for financial gain. Formerly known as Storm-17, Moonstone Sleet has been identified targeting both financial and cyberespionage sectors. Their methods include using trojanized software like PuTTY for initial access, distributing

→ malicious games and Node Package Manager (NPM) packages, deploying custom malware loaders, and creating fake software development companies such as StarGlow Ventures and C.C. Waterfall.

These fake companies engage with potential victims through platforms like LinkedIn, Telegram, freelancing networks, and email.

Pioneer Kitten (Iran-aligned) and Andariel (North Korea-aligned)

These groups have been linked to ransomware attacks, mostly as providers of initial access. They likely sell this access to other cybercriminals for financial gain. The former is mostly breaching sectors like defense, education, finance, and healthcare, while the latter targets critical infrastructure and healthcare organizations, especially in the United States.

Pioneer Kitten also goes by the names Fox Kitten, UNC757, Parisite, RUBIDIUM, and Lemon Sandstorm, and uses a wide range of techniques. Andariel is considered a sub-set of Lazarus Group and has been attributed to North Korea's Reconnaissance General Bureau.

Companies and various organizations are expectedly not the only target for ransomware attacks. Threat actors are once again increasingly exploring and systematically targeting **home users**. In August 2024, Magniber ransomware launched a large-scale global campaign targeting regular end users and encrypting their devices all around the world.

Although such actions have been observed in the past, this campaign marked a significant shift in ransomware targeting strategies mainly because of the scale and wide distribution of the attack which focuses on individual users who often lack robust cybersecurity measures.

Magniber ransomware was distributed through malicious software downloads, fake updates, and key generators, demanding ransoms ranging from $1,000 to $5,000 for decryption. Methods used to distribute Magniber include Windows zero-days, fake Windows and browser updates, and trojanized software cracks and key generators.

Home users must therefore remain vigilant and proactive in their cybersecurity practices. By adopting preventive measures, individuals can significantly reduce their risk of falling victim to ransomware attacks.

Ransom demands targeting individual users increased up to

$5,000

in 2024.
Source: *BleepingComputer: Surge in Magniber ransomware attacks impact home users worldwide*

Prevent More, Manage Less

Ransomware is typically the final payload preceded by other threats including phishing, exploitation, brute force attacks, compromised credentials, downloaders, or custom malware. Many would-be ransomware attacks are caught early in the attack lifecycle, and only if attackers manage to circumvent their victims' defenses and finally attempt to deploy ransomware can we speak about a ransomware attack.

To effectively prevent ransomware attacks, organizations should adopt a multi-layered security approach incorporating automation that addresses each stage of the attack lifecycle. This can be considered a **preventive-first approach** that many organizations and companies increasingly recognize as a strategy with powerful potential—and the reasons are beyond doubt.

First things first: **employee training and awareness** are crucial, as phishing remains one of the primary vectors for ransomware. Employees should be aware of the common signs of phishing and understand the importance of not clicking on unknown links or downloading unsolicited attachments.

Regularly educating staff on recognizing phishing attempts, using strong passwords, and enabling multi-factor authentication can significantly reduce risks. **Endpoint protection** through robust antivirus, anti-malware solutions, and Endpoint Detection and Response (EDR) tools is also important as it is essential for detecting and blocking malicious activities.

No EDR solution is entirely immune to EDR killers, as attackers exploit vulnerabilities in legitimately signed drivers to execute malicious code in kernel space. These drivers, once loaded into Windows, can be used to disable security tools. ESET products effectively block many such vulnerable drivers, and ESET analysts and admins can help customers further strengthen their defenses. By configuring strict PUA settings, only the newest drivers are allowed—an approach that benefits from expert guidance.

Hardening the OS with WDAC rules is also important, which only adds up to a long-term prevention strategy that is necessary per se. Such expert guidance can be a game changer when it comes to dealing with EDR killers.

Further steps to master include **network security measures** such as firewalls, Intrusion Detection Systems (IDS), and network segmentation that help control and monitor traffic, prevent unauthorized access, and limit the spread of ransomware.

Hardly any such measure can be executed without regular **patch management** which ensures that all systems and software are up to date with the latest security patches, closing vulnerabilities that attackers could exploit.

67%

of CISOs reported increasing cybersecurity budgets in 2024 compared to 2023.
Source: *IANS, 2024 Security Budget Benchmark Report*

Implementing access controls based on the principle of least privilege and adopting a **zero-trust security model** further minimizes the risk of unauthorized access and belongs nowadays to a common standard within cybersecurity prevention. That is also the case for **regular backups** of critical data, stored offline or in secure cloud environments, that are vital for recovery in case of an attack. These backups should be, of course, regularly tested to ensure their effectiveness.

When speaking about day-to-day operations and how prevention can be useful there, **email security** measures such as filtering and spam protection help with blocking malicious emails and attachments before they reach users. Many incidents still occur because of human error, and emails remain the most prominent attack vectors.

As there are many other applications people use in daily business, **application whitelisting** is of high importance as well. It ensures that only approved applications can run on the network, preventing unauthorized software from executing.

Having a well-developed **incident response plan** and conducting regular drills ensures that organizations are prepared to respond effectively to ransomware attacks.

All these measures help build a robust cybersecurity posture through proactive defense strategies that stem from the understanding that prevention is always better than cure.

Why Not Pay Ransom?

Let's not be naïve—even with a strong preventive approach, a ransomware attack can still happen. Threat actors constantly refine their tactics, exploiting zero-day vulnerabilities, supply chain weaknesses, or human error to bypass even good defenses. But while an attack can be disruptive, it is not an unsolvable situation. Organizations that act swiftly, leverage incident response plans, and rely on secure backups can recover without giving in to extortion. This brings us to a critical point—why paying the ransom is not the right solution.

63%

was the share of ransomware victims that involved law enforcement and avoided paying a ransom in 2024.

Source: *IBM, Cost of a Data Breach Report 2024*

Paying criminals who have encrypted your data means:

- You are validating the business model behind the crime
- You are encouraging further criminal activity by inadvertently funding it
- You are allowing ransomware gangs to research zero-day vulnerabilities and develop new exploits
- You may be hit with future attacks and further demands for money

Paying the ransom poses no guarantee that cybercriminals will provide a working decryption key—after all, there's no way to hold them accountable or take legal action against them. There are several reasons why paying may not lead to data recovery:

- Some data may have been corrupted during encryption, making it unrecoverable
- The provided decryption tool could be bundled with additional malware, malfunction, or be significantly slower than restoring from backups
- There are multiple ways the decryption key delivery process can fail, including bugs in the decryption code, overly complicated encryption scheme, complications in payment processing (especially with cryptocurrencies), or double-extortion tactics demanding additional payments
- The attacker may simply act in bad faith, with no intention of providing a decryption key

In practice, there are typically two main arguments for paying the ransom. The first is the inability to restore the encrypted data from backups, either because backups don't exist, are incomplete, or have been damaged. However, there may be alternatives to paying. Before making any payments, consult with your security software vendor:

(a) to check if a decryption tool is available for the specific ransomware variant, potentially allowing recovery without payment, and

(b) to verify if paying the ransom is known to be ineffective for that particular variant.

The second common argument for paying the ransom is that it's cheaper than restoring from backups. While this might be technically true in terms of time and labor, it remains a fundamentally flawed decision for several reasons.

As mentioned earlier, the promises of decryption are unreliable, there's a high likelihood of being targeted again after making the first payment—remember, you're not dealing with law-abiding individuals—and by paying, you're supporting a criminal operation, ultimately increasing the likelihood of further attacks on others. Paying is sometimes even illegal and one of the reasons is that the attackers might be under sanctions.

How can ESET help with ransomware & remediation?

A **reliable remediation** tool as part of a proactive, prevention-first strategy can be your best defense against tough decisions—whether to invest heavily in data recovery or even consider paying a ransom. With powerful ransomware remediation technology, you stay a few steps ahead.

ESET's Ransomware Remediation is a fully automated security layer within the modern endpoint protection module of the ESET PROTECT Platform. Designed to enhance ransomware defense, it works alongside Ransomware Shield which detects and blocks suspicious behavior. It combines prevention and remediation into one, providing a comprehensive multistage approach to combating encryption.

94%

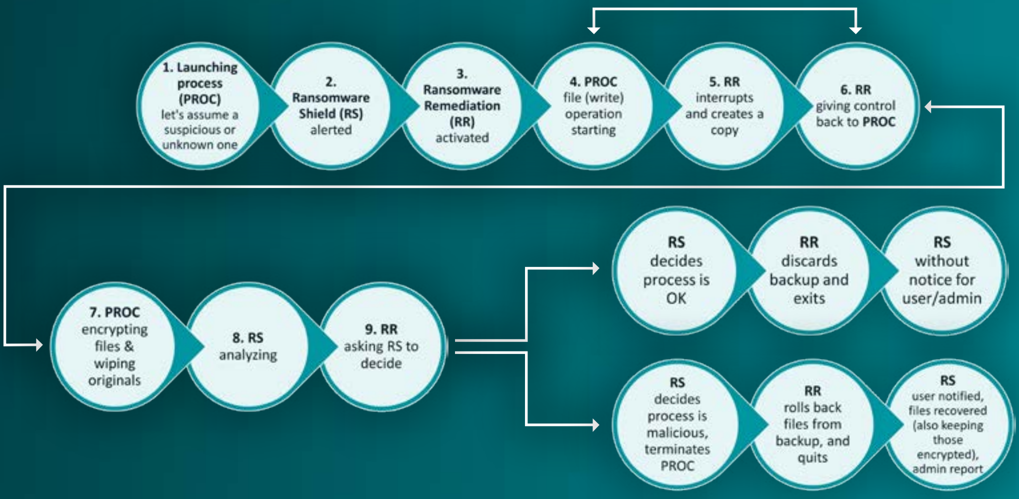
of surveyed organizations reported attempts
by cybercriminals to compromise their backups
during the attack in 2024.
Source: *SC World, Compromised backups send ransomware recovery costs soaring*

Unlike traditional remediation and rollback solutions that rely on the operating system's Volume Shadow Copy Service—often a prime target for attackers—**ESET uses a proprietary file caching solution**, offering greater flexibility and reliability. Ransomware operators frequently delete or overwrite shadow copies to prevent recovery, making traditional rollback methods ineffective.

In contrast, ESET's Ransomware Remediation backup process is not a local service but operates within its **own protected storage section** on the drive where files cannot be modified or corrupted, or deleted by the attackers.

The technology continuously monitors all processes, intercepting file modifications in real time. The moment a file-altering process is detected, ESET's on-the-fly backup system creates copies of the original files—even before behavioral reputation systems like Ransomware Shield determine whether the activity is malicious. It all works in concert with ESET LiveSense technologies, dissecting and analyzing malware to its core.

ESET Ransomware Remediation as a proactive approach ensures that organizations can recover their files instantly, eliminating the need to pay ransom. ESET Ransomware Remediation is included in all ESET PROTECT Platform tiers, starting from ESET PROTECT Advanced. A fully functional 30-day trial is also available.


1. Launching process (PROC) let's assume a suspicious or unknown one
2. Ransomware Shield (RS) alerted
3. Ransomware Remediation (RR) activated
4. PROC file (write) operation starting
5. RR interrupts and creates a copy
6. RR giving control back to PROC
7. PROC encrypting files & wiping originals
8. RS analyzing
9. RR asking RS to decide
RS decides process is OK
RR discards backup and exits
RS without notice for user/admin
RS decides process is malicious, terminates PROC
RR rolls back files from backup, and quits
RS user notified, files recovered (also keeping those encrypted), admin report

ESET Ransomware Shield and Ransomware Remediation's Complex Process Tree

WHAT ARE THE KEY BENEFITS OF ESET'S RANSOMWARE REMEDIATION?

- The tool provides comprehensive rollback through seamless, automated file restoration from secure cache
- It only secures files that are affected by a suspected process, therefore disk space is much less of an issue
- ESET is using its own unique proprietary technology and does not rely on the VSS (Volume Shadow Copy Service) feature provided in Microsoft's Windows Operating Systems, like some other solutions do
- The feature is on by default in eligible ESET PROTECT subscription tiers; there is no user interaction required, and administrators can configure protected folders and file types

Conclusion

Ransomware remains a formidable cybersecurity threat in 2025, with evolving tactics and increasing sophistication. The fall of LockBit and the rise of RansomHub highlights the shifting dynamics of the RaaS ecosystem where success is often measured by the ability to attract and maintain affiliates.

Following LockBit's takedown by law enforcement, many affiliates lost trust and migrated to RansomHub, significantly weakening LockBit's operational scale. Meanwhile, advanced techniques like EDR killers, along with the involvement of APT groups, continue to add layers of complexity to these threats.

Organizations must embrace a multi-layered, preventive-first security approach to effectively combat ransomware and the threats that precede it. This includes employee training, robust endpoint and data protection, regular backups, and advanced security solutions such as MDR* or XDR.

With ESET's comprehensive cybersecurity suite—including Ransomware Remediation technology, a proactive solution allowing you to swiftly recover and minimize the impact of attacks—you can handle even the most sophisticated ransomware threats.

BOOK A DEMO

*Available in select markets.

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

Digital Security
Progress. Protected.