What is ransomware?

By kenwith

Archived: 2026-04-05 22:41:30 UTC

In practice, a *ransomware attack* blocks access to your data until a ransom is paid.

In fact, ransomware is a type of malware or phishing cyber security attack that destroys or encrypts files and folders on a computer, server, or device.

Once devices or files are locked or encrypted, cybercriminals can extort money from the business or device owner in exchange for a *key* to unlock the encrypted data. But even when paid, cybercriminals *might never* give the key to the business or device owner and stop access *permanently*.

Microsoft Security Copilot leverages AI to help mitigate ransomware attacks. For more Microsoft solutions to ransomware, visit our Ransomware solutions library.

Ransomware can be automated or involve human hands on a keyboard - a *human-operated* attack, such as seen in recent attacks using LockBit ransomware.

Human-operated ransomware attacks involve the following stages:

1. **Initial compromise** - The threat actor first gains access to a system or environment following a period of reconnaissance to identify weaknesses in defense.
2. **Persistence and defense evasion** - The threat actor establishes a foothold in the system or environment using a backdoor or other mechanism that operates in stealth to avoid detection by incident response teams.
3. **Lateral movement** - The threat actor uses the initial point of entry to migrate to other systems connected to the compromised device or network environment.
4. **Credential access** - The threat actor uses a fake sign-in page to harvest user or system credentials.
5. **Data theft** - The threat actor steals financial or other data from compromised users or systems.
6. **Impact** - The affected user or organization might suffer material or reputational damage.

- Microsoft Defender XDR - Microsoft Defender XDR includes powerful automated attack disruption capabilities that can protect your environment from sophisticated, high-impact attacks, including human-operated ransomware.
- Microsoft Sentinel - SIEM solution that stops a ransomware attack in its tracks by using machine learning to combine disparate data—network, identity, SaaS, and endpoints from both Microsoft and Partner data sources.
- Security Copilot - During an active ransomware attack, Security Copilot uses machine learning to provide thorough context so security professionals can share clear, concise, and comprehensive summaries of

active incidents. This gives targeted entities a deep understanding of the situation, even when an incident occurs after business hours.

- Qakbot – Uses phishing to spread malicious links, malicious attachments, and to drop malicious payloads like Cobalt Strike Beacon
- Ryuk – Data encryptor typically targeting Windows
- Trickbot – Has targeted Microsoft applications such as Excel and Word. Trickbot was typically delivered via email campaigns that used current events or financial lures to entice users to open malicious file attachments or click links to websites hosting the malicious files. Since 2022, Microsoft's mitigation of campaigns using this malware appears to have disrupted its usefulness.
- LockBit – Financially motivated ransomware-as-a-service (RaaS) campaign and most prolific ransomware threat actor in the 2023-24 time period
- Black Basta – Gains access through spear-phishing emails and uses PowerShell to launch an encryption payload
- Storm-1674 (DarkGate and ZLoader) - Storm-1674 is an access broker known for distributing DarkGate, SectopRAT, and Zloader and handing off access to threat actors like Storm-0506 and Sangria Tempest.

Meanwhile, Storm-1811 is a threat actor known for social engineering attacks leading to the deployment of BlackBasta using Qakbot and other malware. In late October to early November, Storm-1811 was observed flooding target email addresses with spam (email bombing attack) before posing as help desk personnel offering to help with the spam problem. In this new campaign, Storm-1811 was observed deploying a new malware loader called ReedBed.

Microsoft Defender data shows that the most widespread ransomware variants in the last quarter of 2024 were Akira, FOG, Qilin, Lynx, and the aforementioned RansomHub and BlackBasta. This period also saw the new ransomware variants SafePay and Hellcat. March 2025 has seen the resurface of Qilin ransomware through threat actor Moonstone Sleet.

To help mitigate in-progress ransomware attacks, Microsoft Incident Response can leverage and deploy Microsoft Defender for Identity — a cloud-based security solution that helps detect and respond to identity-related threats. Bringing identity monitoring into incident response early supports the affected organization's security operations team to regain control. Microsoft Incident response uses Defender for Identity to help identify the incident scope and impacted accounts, protect critical infrastructure, and evict the threat actor. The response team then brings in Microsoft Defender for Endpoint to trace the threat actor's movements and disrupt their attempts to use compromised accounts to reenter the environment. After containing the incident andregaining and full administrative control over the environment, Microsoft Incident Response collaborates with the customer to help prevent future cyberattacks.

Commodity ransomware attacks are often automated. These cyber attacks can spread like a virus, infect devices through methods like email phishing and malware delivery, and require malware remediation.

Therefore, you can safeguard your email system using Microsoft Defender for Office 365 that protects against malware and phishing delivery. Microsoft Defender for Endpoint works alongside Defender for Office 365 to

automatically detect and block suspicious activity on your devices, while Microsoft Defender XDR detects malware and phishing attempts *early*.

Human-operated ransomware is the result of an **active attack** by cybercriminals that infiltrate an organization's on-premises or cloud IT infrastructure, elevate their privileges, and deploy ransomware to critical data.

These "hands-on-keyboard" attacks usually target organizations rather than a single device.

Human-operated also means there's a human threat actor using their insights into common system and security misconfigurations. They aim to infiltrate the organization, navigate the network, and adapt to the environment and its weaknesses.

Hallmarks of these human-operated ransomware attacks typically include **credential theft** and **lateral movement** with an elevation of the privileges in stolen accounts.

Activities might take place during maintenance windows and involve security configuration gaps discovered by cybercriminals. The goal is the **deployment of a ransomware payload** to whatever *high business impact resources* the threat actors choose.

Important

These attacks can be *catastrophic* to business operations and are difficult to clean up, requiring complete adversary eviction to protect against future attacks. Unlike commodity ransomware that usually only requires malware remediation, **human-operated ransomware will continue to threaten your business operations after the initial encounter**.

Tip

For Azure-specific protection strategies and native capabilities to defend against ransomware in cloud environments, see Ransomware protection in Azure.

The impact and likelihood that human-operated ransomware attacks will continue

First, prevent phishing and malware delivery with Microsoft Defender for Office 365 to protect against malware and phishing delivery, Microsoft Defender for Endpoint to automatically detect and block suspicious activity on your devices, and Microsoft Defender XDR to detect to malware and phishing attempts *early*.

For a comprehensive view of ransomware and extortion and how to protect your organization, use the information in the **Human-Operated Ransomware Mitigation Project Plan** PowerPoint presentation.

1. Assess the situation by analyzing the suspicious activity that alerted your team to the attack.
2. What time/date did you first learn of the incident? What logs are available and is there any indication that the actor is currently accessing systems?
3. Identify the affected line-of-business (LOB) applications, and get any impacted systems back online. Does the affected application require an identity that might have been compromised?

4. Are backups of the application, configuration, and data available and regularly verified using a restore exercise?

5. Determine the compromise recovery (CR) process to remove the threat actor from the environment.

The summary of the guidance in the Human-Operated Ransomware Mitigation Project Plan

- The stakes of ransomware and extortion-based attacks are high.
- However, the attacks have weaknesses that can reduce your likelihood of being attacked.
- There are three steps to configuring your infrastructure to exploit attack weaknesses.

For the three steps to exploit attack weaknesses, see the Protect your organization against ransomware and extortion solution to **quickly** configure your IT infrastructure for the best protection:

1. Prepare your organization to recover from an attack without having to pay the ransom.
2. Limit the scope of damage of a ransomware attack by protecting privileged roles.
3. Make it harder for a threat actor to access your environment by incrementally removing risks.


The three steps to protecting against ransomware and extortion

Download the Protect your organization from ransomware poster for an overview of the three phases as layers of protection against ransomware attacks.


The "Protect your organization from ransomware" poster

Key information from Microsoft:

- The latest ransomware trends from Microsoft, Microsoft latest ransomware blog
- 2024 Microsoft Digital Defense Report Microsoft 365:
- Deploy ransomware protection for your Microsoft 365 tenant

Microsoft Defender XDR:

- Find ransomware with advanced hunting

Microsoft Defender for Cloud Apps:

- Create anomaly detection policies in Defender for Cloud Apps

Microsoft Azure:

- Azure Defenses for Ransomware Attack
- Ransomware protection in Azure

Microsoft Copilot for Security:

- Defend against human-operated ransomware attacks with Microsoft Copilot for Security

OpenAI key ransomware mitigation strategies, in ChatGPT’s own words, include:

1. **Training data curation**
2. **Safety layers and filters**
3. **Empirical testing and red teaming**
4. **Continuous monitoring**
5. **Alignment and safety research**
6. **Community reporting and feedback**
7. **Partnerships and policies**

For more detailed information, refer to OpenAI's official documentation on their approach to AI safety and misuse mitigation.

Microsoft Security ransomware mitigation resources:

See the latest list of ransomware articles in the Microsoft Security Blog.

- Navigating recent ransomware threats (June 2024)
