CS-014 · Malware

Ransomware

Malware that encrypts or blocks access to data and demands payment to restore it.

Executive Summary

Ransomware is malware that encrypts a victim's files or locks their systems and then demands payment, usually in cryptocurrency, in exchange for restoring access. Modern attacks often add a second layer of pressure by stealing data first and threatening to publish it. It is one of the most disruptive and costly threats facing organizations today.

What It Is

Ransomware is a category of malware built around extortion. In the most common form, it encrypts files on a device or across a network so the owner can no longer open them, then displays a ransom note demanding payment for the decryption key. Some variants instead lock the entire screen or device. Ransomware is frequently sold and operated as a service, where developers provide the malware and affiliates carry out the attacks, which has lowered the barrier to entry and increased the volume of attacks. Many campaigns now use double extortion: attackers steal sensitive data before encrypting it and threaten to leak or sell that data if the ransom is not paid, adding pressure even on victims who have good backups.

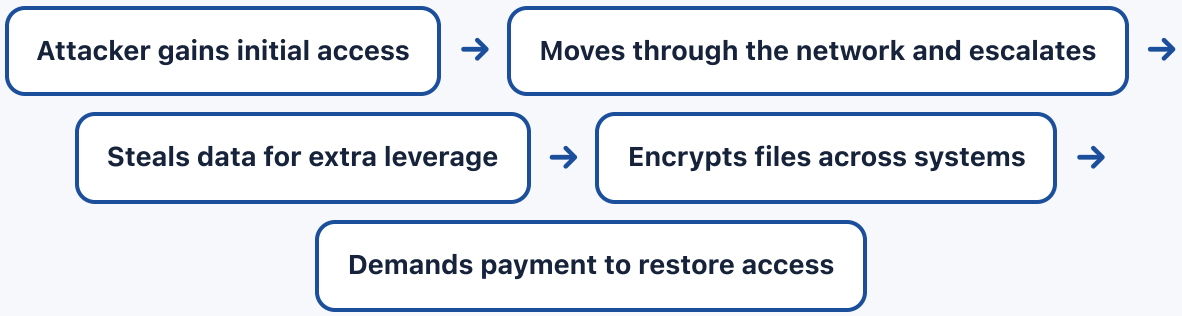
Why It Matters

A ransomware attack can halt an entire organization in hours, taking down operations, cutting off access to critical records, and forcing costly recovery. Beyond the ransom itself, victims face downtime, recovery expenses, potential regulatory exposure from stolen data, and lasting reputational harm. Critical services such as healthcare, government, and infrastructure have been hit, which raises real safety concerns. Paying a ransom carries no guarantee of recovery and may fund further crime, so authorities generally discourage it. This makes prevention, resilient backups, and a tested recovery plan far more valuable than any payment.

How It Works

A ransomware attack usually begins with initial access, often through phishing, stolen credentials, or an exploited vulnerability. The attacker then moves through the network, escalates privileges, and identifies valuable systems and data. In many campaigns they steal data during this stage to enable double extortion. When ready, they deploy the ransomware widely and encrypt files across as many systems as possible, sometimes deleting or disabling backups first to prevent easy recovery. A ransom note then explains how to pay and receive a decryption key. Because so much depends on the early stages, strong access controls, monitoring, and the ability to detect intruders before encryption begins are decisive in limiting damage.

Architecture Diagram



Ransomware follows a path from access to spread to encryption and extortion, with data theft often added for pressure.

Visual Workflow

A ransom note demands payment for the decryption key and to withhold stolen data.

Common Attacks

- Phishing emails that deliver malware or steal the credentials used for access
- Exploitation of unpatched, internet-facing vulnerabilities to break in
- Abuse of exposed or weakly protected remote access services
- Double extortion that steals data before encrypting and threatens to leak it
- Targeting and deleting backups to force victims toward paying

Common Mistakes

- Keeping backups online where the same attack can reach and destroy them
- Never testing whether backups actually restore under pressure
- Leaving remote access exposed without multi-factor authentication
- Delaying patches on internet-facing systems attackers actively target
- Having no incident response plan, so the first response is improvised

Best Practices

- Maintain offline or immutable backups and test restores regularly
- Enforce multi-factor authentication, especially on remote access and email
- Patch promptly, prioritizing internet-facing and remotely exploitable systems
- Apply least privilege and segment networks to limit lateral movement
- Monitor for early intrusion signs before encryption can begin
- Prepare and rehearse a ransomware-specific incident response plan

Quick Checklist

- [ ] Offline or immutable backups in place and restore-tested recently
- [ ] Multi-factor authentication enforced on remote access and email

- [x] Internet-facing systems patched on a defined, prompt schedule
- [x] Least privilege and network segmentation limiting lateral movement
- [x] Monitoring and detection tuned to catch intruders before encryption
- [x] Tested, ransomware-specific incident response and communication plan

Recommended Tools

Endpoint Detection and Response (EDR)
Detects intrusion and ransomware behavior and enables rapid containment

Immutable or offline backup
Provides a recovery path that attackers cannot easily alter or delete

Multi-factor authentication
Blocks the credential abuse used for much ransomware access

Network segmentation
Limits how far ransomware can spread across the environment

Industry Standards

NIST SP 800-61
Incident handling lifecycle for containing and recovering from attacks

NIST SP 800-83
Guidance on preventing and handling malware, including ransomware

CIS Critical Security Controls
Backup, access, and patching safeguards central to ransomware defense

Career Relevance

Ransomware sits at the center of modern security work. Incident responders lead containment and recovery, SOC analysts hunt for the early intrusion signs that precede encryption, and security engineers build the backup, access, and segmentation controls that reduce impact. Malware analysts study ransomware families, and GRC professionals assess resilience and

recovery readiness. For the AI-Governance-Jobs.com audience, ransomware fluency is essential across security and governance roles.

Interview Questions

- What is double extortion, and why does it pressure victims who have backups?
- Why do experts generally advise against paying the ransom?
- What makes offline or immutable backups so important for ransomware recovery?
- How does an attacker typically progress from initial access to encryption?
- What early warning signs might a SOC catch before ransomware detonates?

Related Certifications

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | GIAC Reverse Engineering Malware (GREM)

Further Reading

- CISA StopRansomware
- NIST SP 800-61: Computer Security Incident Handling Guide
- MITRE ATT&CK

Key Takeaways

- Ransomware encrypts or locks data and demands payment to restore access.
- Modern attacks often steal data first for double extortion.
- Paying does not guarantee recovery and may fund more crime.
- Offline or immutable, tested backups are the strongest recovery control.
- Prevention and early detection before encryption limit the most damage.

FAQ

▶ **Should an organization pay the ransom?**

▶ **What is double extortion?**

▶ **What is the single most important defense?**

Related Careers

RELATED ROLES

Incident Responder | Soc Analyst | Security Engineer

RELATED CERTIFICATIONS

CompTIA Security+

ISC2 Certified in Cybersecurity (CC)

GIAC Reverse Engineering Malware (GREM)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Ransomware**
3. Go deeper: Computer Viruses
4. Go deeper: Trojans
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-011 Computer Viruses | CS-012 Trojans | CS-013 Worms | CS-001 Cybersecurity | CS-081 Patch Management