

No. 94

CYBERSECURITY

Ransomware

How ransomware works and how to prevent, survive and recover



oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 94

Ransomware

How ransomware works and how to prevent, survive and recover

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Ransomware

How ransomware works and how to prevent, survive and recover

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product, company and group names mentioned in this book are trademarks or names of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · UNDERSTANDING RANSOMWARE

1 What ransomware is 5
2 A short history 7
3 Ransomware by the numbers 9
4 The ransomware business 11
5 Extortion tactics 13

PART II · HOW ATTACKS HAPPEN

6 How ransomware gets in 16
7 Inside an attack 18
8 Who gets targeted 20
9 Lessons from well-known attacks 21

PART III · PREVENTION AND PREPARATION

10 Layered defence 24
11 Patching and exposure 26
12 Protecting identities 27
13 Email and user defences 29
14 Segmentation and least privilege 30
15 Backups that survive 31
16 Detection and early warning 33
17 Virtualization, cloud and SaaS 34
18 Planning and practice 35

PART IV · RESPONSE AND RECOVERY

19 The first hours 37
20 The ransom decision 39
21 Recovery 41
22 Communication and legal duties 42

FREE SAMPLE · ojayo.com

23 Lessons learned 43
24 Cyber insurance 44
25 A readiness plan 45
Checklists 46
Glossary 47
Further reading 48

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Ransomware is malicious software that locks an organization's files and systems until a ransom is paid, and today it almost always comes with data theft and threats to publish what was stolen. It is one of the most damaging cyber threats in the world: it has closed hospitals, halted factories and shut down schools and city councils.

This book explains ransomware for beginners: how the criminal business works, how attacks unfold, and above all how to prevent attacks, detect them early and recover if one succeeds. It is written for defenders and contains no instructions for building or using ransomware.

What this book covers

- What ransomware is, its history and the criminal economy behind it.
- How attackers get in and what they do before encrypting.
- Prevention: patching, identity, email security and segmentation.
- Backups that survive an attack, detection and early warning signs.
- Responding, the ransom decision, recovery and lessons learned.

Who this book is for

- **IT staff and beginners in security.**
- **Business owners and managers** who must plan for an attack.
- **Anyone** who wants to understand one of the biggest threats in the news.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Understanding ransomware** (Chapters 1–5): what it is, a short history, the numbers, the business model and extortion tactics.
- **Part II — How attacks happen** (Chapters 6–9): ways in, inside an attack, who gets targeted, and lessons from well-known attacks.
- **Part III — Prevention and preparation** (Chapters 10–18): layered defence, patching, identity, email, segmentation, backups, detection, virtualization and cloud, and planning.
- **Part IV — Response and recovery** (Chapters 19–25): the first hours, the ransom decision, recovery, communication and legal duties, lessons learned, cyber insurance, and a readiness plan.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How an idea looks in a real situation.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on facts and screens

Statistics are named with their source; ransomware figures vary widely by how they are measured, so compare like with like. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Understanding ransomware

These chapters explain what ransomware is, where it came from, how big the problem is and how the criminal business behind it works.

FREE SAMPLE · ojayo.com

CHAPTER 1

What ransomware is

Ransomware locks your systems and steals your data to force a payment.

The basic idea

Ransomware **encrypts** files, scrambling them with a key only the attacker holds, and then demands payment, usually in cryptocurrency, for the key to unlock them.



Figure 1.1 Ransomware in five steps

Modern ransomware is human-operated

Most serious attacks today are not automatic infections. People, often helped by automated tools and AI, break in, explore the network for days, steal data, disable defences and then encrypt as many systems as they can at once.

Who is affected

Any organization can be hit: hospitals, schools, manufacturers, councils, law firms and small businesses. Attackers choose targets that rely heavily on their systems and are likely to pay.

FREE SAMPLE · ojayo.com

Ransom note (simplified, fictional example)

Illustration, not an actual product screen

NOTICE

Your files are encrypted

72:00:00

Claim	Reality
Pay to get the decryptor	decryptors often slow or faulty
We will delete your data	no way to verify
Do not contact police	pressure tactic; report anyway
Price doubles in 72 hours	urgency to stop you thinking

Figure 1.2 What a ransom note claims, and the reality

KEY IDEA

Ransomware is the final step of a break-in. Stop the break-in and you stop the ransomware.

FREE SAMPLE · ojayo.com

CHAPTER 2

A short history

Ransomware has evolved from a curiosity to a global criminal industry.



Figure 2.1 A short history of ransomware

Early days

The 1989 "AIDS Trojan" was distributed on floppy disks and demanded payment by post. For two decades ransomware remained a minor problem.

The cryptocurrency era

From 2013, families such as **CryptoLocker** used strong encryption and Bitcoin payments, making ransomware profitable. In 2017 **WannaCry** spread worldwide in days, hitting organizations including parts of the UK's National Health Service.

Double extortion and big-game hunting

From 2019 criminals began stealing data before encrypting and threatening to publish it on **leak sites**. They also shifted to "big-game hunting": targeting large organizations for large ransoms.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware (you are reading this)
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Ransomware

Enjoyed it? The full book has 53 pages and 25 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.