

No. 124

CYBERSECURITY

Malware Analysis Basics

Understanding malicious software safely, for defenders

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 124

Malware Analysis Basics

Understanding malicious software safely, for defenders

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Malware Analysis Basics
Understanding malicious software safely, for defenders

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 and tool names mentioned in this book are trademarks 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 · FOUNDATIONS

1 What malware is 5
2 Kinds of malware 6
3 Malware families and naming 7
4 How malware spreads 8
5 Why defenders analyse malware 9
6 Levels of analysis 10
7 Safety and ethics 11
8 Legal considerations 12
9 Building a lab 13
10 Handling and storing samples 14

PART II · ANALYSIS

11 Triage 16
12 File types 17
13 Static analysis 18
14 Hashes in practice 19
15 Strings 20
16 Packing and obfuscation 21
17 Sandboxes 22
18 Network behaviour 23
19 Dynamic analysis 24
20 Memory analysis 25
21 Reverse engineering, briefly 26

PART III · FROM FINDINGS TO DEFENCE

22 Indicators of compromise 28
23 Behaviours 29

FREE SAMPLE · ojayo.com

24 The Pyramid of Pain 30
25 Detection rules 31
26 A first detection rule 32
27 Scoping 33
28 Reporting 34
29 Sharing 35

PART IV · PRACTICE

30 Tools 37
31 AI assistance 38
32 Mapping to MITRE ATT&CK 39
33 Evasion 40
34 Malicious documents and scripts 41
35 Careers 42
36 Common mistakes 43
37 A worked example 44
38 A learning path 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.

Malware, malicious software, is behind ransomware attacks, stolen passwords, spying and fraud. When a suspicious file turns up, defenders need to answer questions quickly: Is it malicious? What does it do? Has it spread? How do we detect and remove it? **Malware analysis** answers those questions.

This book introduces malware analysis for beginners, entirely from a defender's perspective. It explains the kinds of malware, how to build a safe lab, how to triage samples, the basics of static and dynamic analysis, how to turn findings into detections and how to share results. It does not teach how to write or deploy malware.

What this book covers

- Kinds of malware and how they work at a high level.
- Why and when defenders analyse malware.
- Safety, legal considerations and building an isolated lab.
- Triage, static analysis and dynamic analysis basics.
- Indicators, behaviours, detection rules and reporting.
- Tools, AI-assisted analysis and a learning path.

Who this book is for

- **SOC analysts and incident responders.**
- **Students** interested in malware research.
- **IT staff** who want to understand threats.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–10): what malware is, kinds and families of malware, how it spreads, why analyse, levels of analysis, safety and ethics, legal considerations, the lab, and sample handling.
- **Part II — Analysis** (Chapters 11–21): triage, file types, static analysis, strings, packing and obfuscation, sandboxes, dynamic analysis, memory, and an introduction to reverse engineering.
- **Part III — From findings to defence** (Chapters 22–29): indicators, behaviours, the Pyramid of Pain, detection rules, scoping, reporting, and sharing.
- **Part IV — Practice** (Chapters 30–38): tools, AI assistance, evasion, malicious documents and scripts, careers, common mistakes, a worked example, and a learning path.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How an idea looks in real analysis work.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on safety

Real malware can damage systems and spread. Only handle samples in an isolated lab, follow your organization's policies and never run suspicious files on work or personal computers. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what malware is, why defenders analyse it, and how to do so safely.

FREE SAMPLE · ojayo.com

CHAPTER 1

What malware is

Malware is software designed to cause harm.

A definition

Malware is any software intentionally designed to harm, steal, spy, disrupt or gain unauthorized access. It can be an executable file, a script, a malicious document, a browser extension or code that only ever runs in memory.

A criminal industry

Much malware is developed and sold as a service: developers rent infostealers, loaders and ransomware to other criminals, who use them in campaigns.

> **KEY IDEA**
> Understanding malware helps you find it, stop it and recover faster.

FREE SAMPLE · ojayo.com

CHAPTER 2

Kinds of malware

Malware comes in many forms.

Type	What it does
Ransomware	encrypts files, demands payment
Infostealer	steals passwords, cookies, wallets
Remote access trojan	gives attackers control
Loader or dropper	installs other malware
Worm	spreads by itself
Rootkit	hides deep in the system
Crypto-miner	uses your computing power

Figure 2.1 Common kinds of malware

Combinations

Real attacks often chain several kinds: a phishing document drops a loader, which installs an infostealer and later ransomware.

FREE SAMPLE · ojayo.com

CHAPTER 3

Malware families and naming

Analysts group malware into families.

Families

A **family** is a group of samples sharing the same code base, such as many versions of one infostealer. Recognizing the family tells you what to expect: its usual capabilities, persistence and targets.

Why names differ

Security vendors often give the same family different names, because each discovered and labelled it independently. Threat intelligence platforms and MITRE ATT&CK's software list help map names to one another.

Variants

Attackers constantly release new **variants**, slightly changed versions that produce new hashes. This is why detection based on behaviour matters more than detection based on a single file.

> **TIP**
> When a report names a family, check two or three sources before assuming you know exactly what it does.

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
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 (you are reading this)
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

Malware Analysis Basics

Enjoyed it? The full book has 53 pages and 38 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.