Training Course on Ransomware Analysis and Decryption Challenges

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

With the exponential growth of ransomware attacks targeting critical infrastructure, hospitals, educational institutions, and private businesses, there is an urgent need for skilled professionals capable of understanding, analyzing, and countering these threats. Training Course on Ransomware Analysis and Decryption Challenges is designed to equip cybersecurity analysts, incident responders, and digital forensic experts with the latest tools, methodologies, and strategies to mitigate, analyze, and decrypt ransomware strains. This course emphasizes real-world ransomware variants, cyber threat intelligence, reverse engineering, decryption mechanisms, and threat actor profiling.

Participants will gain hands-on experience with live ransomware samples, simulate infection chains, extract IOCs (Indicators of Compromise), and apply memory forensics, registry analysis, and cryptographic attack techniques to attempt decryption. The curriculum also explores current trends such as Ransomware-as-a-Service (RaaS) and double extortion tactics, bridging the gap between theory and field application through practical labs and case studies.

Programme Curriculum

Training Course on Ransomware Analysis and Decryption Challenges

Introduction

With the exponential growth of ransomware attacks targeting critical infrastructure, hospitals, educational institutions, and private businesses, there is an urgent need for skilled professionals capable of understanding, analyzing, and countering these threats. Training Course on Ransomware Analysis and Decryption Challenges is designed to equip cybersecurity analysts, incident responders, and digital forensic experts with the latest tools, methodologies, and strategies to mitigate, analyze, and decrypt ransomware strains. This course emphasizes real-world ransomware variants, cyber threat intelligence, reverse engineering, decryption mechanisms, and threat actor profiling.

Participants will gain hands-on experience with live ransomware samples, simulate infection chains, extract IOCs (Indicators of Compromise), and apply memory forensics, registry analysis, and cryptographic attack techniques to attempt decryption. The curriculum also explores current trends such as Ransomware-as-a-Service (RaaS) and double extortion tactics, bridging the gap between theory and field application through practical labs and case studies.

Course Objectives

1. Understand the evolving landscape of ransomware and major global trends.
2. Analyze ransomware execution flows using static and dynamic malware analysis.
3. Use advanced forensic tools for memory and disk analysis.
4. Reverse engineer ransomware binaries to identify encryption algorithms.
5. Apply cryptographic concepts to understand ransomware key structures.
6. Utilize sandbox environments to observe ransomware behavior safely.
7. Extract IOCs for proactive defense and threat hunting.
8. Analyze encrypted file samples and identify attack vectors.
9. Investigate ransomware notes, payment channels, and actor signatures.
10. Deploy decryption tools and analyze their effectiveness and limitations.
11. Assess Ransomware-as-a-Service (RaaS) operations and affiliate models.
12. Understand legal, ethical, and organizational implications of ransomware response.
13. Apply real-time case studies for hands-on ransomware mitigation strategies.

Target Audiences

1. Cybersecurity Analysts
2. Incident Responders
3. Digital Forensics Experts
4. Penetration Testers
5. IT Security Administrators
6. Law Enforcement Cyber Units
7. SOC Teams
8. Cybersecurity Students/Interns

Course Duration: 10 days

Course Modules

Module 1: Introduction to Ransomware and Threat Landscape

- History of ransomware and evolution
- Modern ransomware families overview
- Motivations behind ransomware attacks
- Ransomware economics and dark web trends
- Government responses and legal considerations
- **Case Study**: Colonial Pipeline Attack Analysis

Module 2: Ransomware Execution Flow

- Initial infection vectors
- Payload deployment methods
- Persistence mechanisms
- File encryption and deletion patterns
- Communication with C2 servers
- **Case Study**: Ryuk Ransomware Behavioral Flow

Module 3: Static and Dynamic Malware Analysis

- Disassemblers and debuggers (Ghidra, IDA Pro)
- Behavioral analysis with sandboxes
- Obfuscation and packing techniques
- String extraction and file structure mapping
- Identifying malicious APIs and system calls
- **Case Study**: Analysis of STOP/Djvu Family

Module 4: Cryptographic Fundamentals for Decryption

- Symmetric vs. asymmetric encryption
- RSA, AES, and hybrid models used in ransomware
- Key generation and management
- Brute-force vs. known-plaintext attacks
- Weak implementations and cryptographic flaws
- **Case Study**: TeslaCrypt Key Recovery

Module 5: Memory Forensics and Ransomware

- Volatility framework usage
- Capturing memory dumps
- Recovering encryption keys from memory
- Malware injection and unpacking
- Detecting running ransomware processes
- **Case Study**: Memory Key Recovery of WannaCry

Module 6: Registry and File System Analysis

- Persistence keys in Windows registry
- Prefetch, RecentDocs, and link files
- Log file correlation
- Shadow copies and volume snapshots
- Recovering encrypted file metadata
- **Case Study**: REvil Registry Forensics

Module 7: Indicators of Compromise and Threat Hunting

- IOC types: hashes, IPs, domains, mutexes
- Correlation with SIEM tools
- Threat intelligence feeds
- Signature vs. behavior-based detection
- Threat mapping using MITRE ATT&CK
- **Case Study**: IOC Development for Maze

Module 8: Reverse Engineering Ransomware Samples

- Understanding compiled binaries
- Decompilation workflows
- Unpacking techniques and bypasses
- Debugging runtime behaviors
- Identifying custom cryptographic routines
- **Case Study**: Reverse Engineering Cerber

Module 9: Ransomware Decryption Tools and Limitations

- Open-source vs. proprietary decryptors
- Using NoMoreRansom.org tools

- Limitations in brute-force decryption
- Decryptor testing labs
- Forensics chain of custody during decryption
- **Case Study**: Successful Decryption with Emsisoft

Module 10: Ransomware as a Service (RaaS) Ecosystem

- Understanding the affiliate model
- Dark web advertisement and recruitment
- Revenue sharing and encryption modules
- Monitoring RaaS marketplaces
- Investigative techniques for takedown
- **Case Study**: DarkSide Affiliate Structure

Module 11: Double Extortion and Data Leaks

- What is double extortion?
- Leak sites and negotiation platforms
- Exfiltration before encryption
- Legal implications of paying ransoms
- Data breach notification laws
- **Case Study**: Clop Ransomware Extortion Strategy

Module 12: Incident Response Planning

- Creating ransomware-specific playbooks
- Role of SOC and CERT teams
- Backup and restore best practices
- Isolation and containment procedures
- Communication with stakeholders and media
- **Case Study**: Organizational Response Simulation

Module 13: Legal and Ethical Dimensions

- Ransom payment legality
- Reporting requirements and disclosures
- GDPR and HIPAA implications
- Ethics of hacking back
- Working with law enforcement
- **Case Study**: Ethical Dilemma in Ransom Payment

Module 14: Post-Incident Recovery and Lessons Learned

- Restoring systems securely
- Vulnerability assessment
- Employee awareness and training
- Updating threat models and policies
- Continuous monitoring post-incident
- **Case Study**: Post-Mortem of JBS Attack

Module 15: Future of Ransomware and Defense Trends

- AI-driven ransomware evolution
- Quantum cryptography threats
- Zero trust and XDR integration
- Predictive threat modeling

- Automation in detection and response
- **Case Study**: Predicting Future RaaS Models

Training Methodology

- Interactive instructor-led sessions
- Virtual lab environments with real ransomware samples
- Group-based case study analysis
- Hands-on reverse engineering and decryption exercises
- Knowledge checks and quizzes after each module
- Final capstone ransomware analysis project

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com