Training Course on Analyzing Advanced Persistent Threat (APT) Malware

Professional Development Training Course Outline

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

Course Introduction

In today’s cyber-threat landscape, Advanced Persistent Threats (APTs) represent some of the most complex, targeted, and damaging forms of malware attacks. These stealthy and prolonged attacks are typically carried out by nation-state actors, cybercriminal groups, or industrial spies, often targeting sensitive government, financial, and corporate data. As organizations shift to hybrid infrastructures, understanding the tactics, techniques, and procedures (TTPs) of APT groups is no longer optional—it's mission-critical. Training Course on Analyzing Advanced Persistent Threat (APT) Malware is designed to equip cybersecurity professionals with advanced skills to detect, analyze, and mitigate APT malware using cutting-edge threat intelligence tools and reverse engineering techniques.

This training delivers a hands-on, lab-intensive experience that goes beyond surface-level analysis to explore real-world APT scenarios, threat hunting strategies, and malware behavior profiling. Learners will gain proficiency in indicators of compromise (IOCs), YARA rule creation, sandboxing, memory forensics, and network traffic analysis. Each module includes real APT case studies—such as APT28, Lazarus Group, and Hafnium—to reinforce practical skills. This course empowers security analysts, incident responders, malware reverse engineers, and threat hunters to detect and respond to persistent threats effectively and proactively.

Programme Curriculum

Training Course on Analyzing Advanced Persistent Threat (APT) Malware

Introduction

In today’s cyber-threat landscape, Advanced Persistent Threats (APTs) represent some of the most complex, targeted, and damaging forms of malware attacks. These stealthy and prolonged attacks are typically carried out by nation-state actors, cybercriminal groups, or industrial spies, often targeting sensitive government, financial, and corporate data. As organizations shift to hybrid infrastructures, understanding the tactics, techniques, and procedures (TTPs) of APT groups is no longer optional—it's mission-critical. Training Course on Analyzing Advanced Persistent Threat (APT) Malware is

designed to equip cybersecurity professionals with advanced skills to detect, analyze, and mitigate APT malware using cutting-edge threat intelligence tools and reverse engineering techniques.

This training delivers a hands-on, lab-intensive experience that goes beyond surface-level analysis to explore real-world APT scenarios, threat hunting strategies, and malware behavior profiling. Learners will gain proficiency in indicators of compromise (IOCs), YARA rule creation, sandboxing, memory forensics, and network traffic analysis. Each module includes real APT case studies—such as APT28, Lazarus Group, and Hafnium—to reinforce practical skills. This course empowers security analysts, incident responders, malware reverse engineers, and threat hunters to detect and respond to persistent threats effectively and proactively.

Course Objectives

1. Understand the lifecycle and strategies of Advanced Persistent Threat (APT) campaigns
2. Identify malware infection vectors used in targeted attacks
3. Perform advanced behavioral and static malware analysis
4. Use YARA rules and Sigma rules for threat hunting and detection
5. Reverse engineer malware using Ghidra, IDA Pro, and x64dbg
6. Analyze APT command-and-control (C2) communications and exfiltration tactics
7. Utilize MITRE ATT&CK framework to map adversary behaviors
8. Examine fileless malware and memory-resident payloads
9. Perform network traffic analysis using Wireshark and Zeek
10. Apply digital forensics to discover APT persistence mechanisms
11. Generate threat intelligence reports from malware indicators
12. Detect rootkits and stealth malware using memory forensics
13. Build and automate malware analysis pipelines using open-source tools

Target Audience

1. Cybersecurity Analysts
2. Incident Response Teams
3. Malware Reverse Engineers
4. Threat Intelligence Analysts
5. SOC Analysts
6. Government Cyber Units
7. Penetration Testers
8. Information Security Officers

Course Duration: 10 days

Course Modules

Module 1: Introduction to APT Malware

- APT lifecycle and objectives
- Common APT threat actors
- Historical evolution of APTs
- Indicators of compromise (IOCs)
- Understanding threat actor motivations
- **Case Study**: APT29’s SolarWinds attack

Module 2: Malware Classification and Taxonomy

- Types of malware used in APTs
- Obfuscation and packing techniques
- Categorizing malware behaviors

- Fileless vs traditional malware
- Use of droppers and loaders
- **Case Study**: Lazarus Group’s RAT variants

Module 3: Static Malware Analysis Techniques

- Hashing and signature detection
- PE file structure analysis
- Strings and metadata extraction
- Identifying obfuscation layers
- Use of tools like PEStudio and Detect It Easy
- **Case Study**: Reverse engineering Turla’s payload

Module 4: Dynamic Malware Analysis

- Setting up a malware sandbox
- Behavior monitoring tools (Procmon, Regshot)
- API call analysis
- Network simulation for safe detonation
- Behavioral IOC generation
- **Case Study**: Sandboxing APT32’s dropper

Module 5: Malware Reverse Engineering

- Assembly language essentials
- Disassembly with IDA Pro
- Debugging with x64dbg
- Code decryption techniques
- Extracting hardcoded C2 info
- **Case Study**: Ghidra analysis of APT41 malware

Module 6: YARA Rules and IOC Development

- Writing custom YARA rules
- Identifying malware patterns
- File and memory scanning
- Sigma rule mapping
- Integration with SIEM tools
- **Case Study**: Creating YARA rules for APT33

Module 7: Command and Control (C2) Analysis

- DNS tunneling and HTTPS C2
- Beaconing patterns
- Extracting C2 indicators
- Detecting encrypted payloads
- Tactics for takedown and disruption
- **Case Study**: Disrupting FIN7’s infrastructure

Module 8: Threat Hunting with MITRE ATT&CK

- Navigating the MITRE ATT&CK matrix
- Mapping APT TTPs to ATT&CK techniques
- Correlating logs with TTPs
- Identifying behavior anomalies
- Adversary emulation tools (CALDERA, Atomic Red Team)

- **Case Study**: Mapping APT10 attack lifecycle

Module 9: Memory Forensics and Fileless Malware

- Volatility framework for analysis
- Detection of injected code
- Analyzing memory dumps
- Spotting hollowing and reflective loading
- Memory-resident malware behavior
- **Case Study**: Fileless malware used by APT38

Module 10: Network Traffic and PCAP Analysis

- Capturing and analyzing PCAPs
- Identifying exfiltration channels
- Decryption techniques for traffic
- Using Zeek and Suricata
- Correlating anomalies with endpoints
- **Case Study**: Network behavior of APT34

Module 11: Persistence and Lateral Movement

- Registry persistence techniques
- DLL side-loading and COM hijacking
- Scheduled tasks and WMI abuse
- Pass-the-Hash and credential dumping
- Pivot detection strategies
- **Case Study**: Lateral movement by APT1

Module 12: APT Threat Intelligence Reporting

- Data enrichment and context
- Report structuring and STIX/TAXII usage
- MISP and threat intel sharing
- Visualizing threat actor timelines
- Communicating findings to executives
- **Case Study**: Reporting on APT12 activity

Module 13: Detection Engineering and Automation

- SIEM integration and alerting
- Automated sandbox detonation
- Leveraging APIs for analysis
- Pipeline building with Python and Docker
- Continuous threat detection models
- **Case Study**: Building APT detection pipelines

Module 14: Red vs Blue Simulation for APTs

- Emulating APT campaigns in lab
- Purple team collaboration
- Adversary emulation tools
- Blue team detection challenges
- Offensive-defensive alignment
- **Case Study**: Simulating APT37 techniques

Module 15: Capstone Lab and Assessment

- Full APT scenario investigation
- Malware analysis report submission
- Threat hunting and IOC extraction
- C2 communication tracing
- Group debrief and feedback
- **Case Study**: End-to-end analysis of Hafnium

Training Methodology

- Hands-on virtual labs with malware samples
- Real-world APT case study walkthroughs
- Daily debriefs and threat actor discussions
- Access to reverse engineering tools and virtualized environments
- Final assessment with practical malware analysis tasks

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org 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
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now

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