Training Course on Malware Campaign Tracking and Attribution

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$2,200 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s digital battlefield, the ability to track and attribute malware campaigns is a critical skill for cybersecurity professionals. With the increasing sophistication of Advanced Persistent Threats (APTs), nation-state actors, and cybercriminal groups, organizations must deploy cutting-edge tools and methodologies to identify, monitor, and respond to malicious campaigns. Training Course on Malware Campaign Tracking and Attribution equips participants with tactical knowledge and practical techniques for malware reverse engineering, infrastructure pivoting, behavioral analytics, threat actor profiling, and intelligence enrichment for attribution.

The course integrates real-world threat intelligence feeds, advanced malware analysis, and network traffic forensics to provide a comprehensive understanding of how threat actors operate. Learners will explore indicators of compromise (IOCs), TTPs (tactics, techniques, and procedures), and the MITRE ATT&CK framework. Participants will also gain experience using threat attribution models, mapping threat infrastructure, and leveraging OSINT and commercial threat intelligence platforms to track malware campaigns in the wild.

Programme Curriculum

Training Course on Malware Campaign Tracking and Attribution

Introduction

In today’s digital battlefield, the ability to track and attribute malware campaigns is a critical skill for cybersecurity professionals. With the increasing sophistication of Advanced Persistent Threats (APTs), nation-state actors, and cybercriminal groups, organizations must deploy cutting-edge tools and methodologies to identify, monitor, and respond to malicious campaigns. Training Course on Malware Campaign Tracking and Attribution equips participants with tactical knowledge and practical techniques for malware reverse engineering, infrastructure pivoting, behavioral analytics, threat actor profiling, and intelligence enrichment for attribution.

The course integrates real-world threat intelligence feeds, advanced malware analysis, and network traffic forensics to provide a comprehensive understanding of how threat actors operate. Learners will explore indicators of compromise (IOCs), TTPs (tactics, techniques, and procedures), and the MITRE ATT&CK framework. Participants will also gain experience using threat attribution models, mapping threat infrastructure, and leveraging OSINT and commercial threat intelligence platforms to track malware campaigns in the wild.

Course Objectives

By the end of this course, learners will be able to:

1. Identify and analyze malware campaign infrastructure and delivery mechanisms.
2. Understand common malware families, their signatures, and behaviors.
3. Apply threat hunting techniques to uncover ongoing malware activity.
4. Use OSINT tools for threat actor profiling and campaign linkage.
5. Map campaigns to the MITRE ATT&CK framework and develop attribution hypotheses.
6. Utilize sandboxing environments for malware detonation and dynamic analysis.
7. Conduct static and behavioral malware analysis to extract IOCs.
8. Correlate network traffic and host artifacts with known threat actor patterns.
9. Apply forensic techniques to identify persistence and exfiltration tactics.
10. Leverage commercial and community threat intelligence platforms for enrichment.
11. Develop detailed attribution reports supported by evidence-based findings.
12. Simulate and track phishing, loader, and dropper malware campaigns.
13. Integrate malware tracking data into SIEMs for real-time alerting.

Target Audience

1. Cybersecurity Analysts
2. Threat Intelligence Professionals
3. Incident Responders
4. SOC Team Members
5. Digital Forensics Experts
6. Malware Reverse Engineers
7. Cybercrime Investigators
8. Government & Law Enforcement Agencies

Course Duration: 10 days

Course Modules

Module 1: Introduction to Malware Campaigns

- Understanding malware lifecycle and architecture
- Classification of malware types and delivery vectors
- Overview of known campaigns and attribution challenges
- Key players: APT groups and cybercrime syndicates
- Tools used in malware campaigns
- **Case Study:** Analysis of the SolarWinds Orion Supply Chain Attack

Module 2: Campaign Infrastructure & Delivery Analysis

- Command & Control (C2) infrastructure mapping
- Domain generation algorithms (DGAs)
- Payload delivery through phishing and drive-by downloads
- Exploit kits and watering hole attacks
- Malware distribution channels on the dark web

- **Case Study:** Emotet malware campaign infrastructure

Module 3: Static and Dynamic Malware Analysis

- Binary unpacking and deobfuscation techniques
- Signature detection using YARA rules
- Sandboxing and behavioral observation
- Registry, file system, and memory analysis
- Tools: IDA Pro, Ghidra, Cuckoo Sandbox
- **Case Study:** TrickBot malware reverse engineering

Module 4: IOC Extraction and Enrichment

- Extracting domains, hashes, IPs, and mutexes
- IOC correlation with threat intelligence feeds
- IOC scoring and prioritization
- Threat feed integration: VirusTotal, AlienVault OTX
- IOC lifecycle management
- **Case Study:** IOC mapping in a ransomware campaign

Module 5: MITRE ATT&CK Mapping

- Understanding tactics, techniques, and procedures (TTPs)
- Mapping malware behavior to MITRE ATT&CK
- Building threat intelligence profiles
- Leveraging ATT&CK Navigator for campaign visualization
- Mitigation strategies based on mapping
- **Case Study:** Mapping APT29 campaign to MITRE ATT&CK

Module 6: Threat Actor Profiling

- Threat actor motivation and capability analysis
- Language, toolkits, and infrastructure reuse
- Profiling based on campaign signatures
- Behavioral and timeline-based profiling
- Mapping to known threat actor groups
- **Case Study:** Lazarus Group attribution analysis

Module 7: Threat Hunting for Active Campaigns

- Identifying anomalies in logs and network traffic
- Using Splunk, ELK, and custom scripts
- Behavior-based hunting with Sigma rules
- Threat hunting playbooks and workflows
- Real-time alert generation from tracked campaigns
- **Case Study:** Hunting QakBot in enterprise networks

Module 8: Network and Endpoint Forensics

- Packet capture and traffic analysis using Wireshark
- Endpoint behavior tracking with EDR tools
- Lateral movement detection techniques
- Persistence and privilege escalation indicators
- Timeline creation and event correlation
- **Case Study:** Analysis of the NotPetya campaign spread

Module 9: Attribution Techniques and Models

- Attribution lifecycle and evidentiary standards
- Technical, strategic, and geopolitical attribution
- The Diamond Model of Intrusion Analysis
- Confidence scoring and hypothesis development
- Avoiding false attribution pitfalls
- **Case Study:** Attribution of Stuxnet

Module 10: OSINT for Campaign Tracking

- Passive DNS, WHOIS, and certificate transparency logs
- Social media and underground forum monitoring
- Github, Pastebin, Telegram as intelligence sources
- Recon-ng, Maltego, and Shodan use cases
- OSINT sanitization and legal considerations
- **Case Study:** Tracking TA505 infrastructure using OSINT

Module 11: Commercial Threat Intelligence Platforms

- Overview of Recorded Future, Mandiant, Anomali, ThreatConnect
- Platform integrations with SIEMs and SOARs
- Threat scoring and enrichment APIs
- Custom dashboard development
- Data ingestion and visualization
- **Case Study:** Using Mandiant to track FIN7

Module 12: Malware Family Deep Dives

- In-depth exploration of prominent malware families
- TTP comparison across variants
- Evolution and version analysis
- Decoder script creation and adaptation
- Understanding loader-dropper relationships
- **Case Study:** REvil ransomware family breakdown

Module 13: Campaign Simulation & Red Team Insights

- Simulating phishing and malware dropper campaigns
- Red vs Blue team perspectives on campaign tracking
- Generating synthetic IOCs
- Campaign simulation frameworks (e.g., Infection Monkey)
- Purple teaming for attribution exercises
- **Case Study:** Simulated spear-phishing and analysis

Module 14: Attribution Report Writing

- Structuring attribution reports for executive and technical audiences
- Integrating visualizations and IOC evidence
- Addressing attribution confidence and caveats
- Recommendations and mitigation planning
- Peer review and dissemination techniques
- **Case Study:** Attribution report on DarkHydrus campaign

Module 15: Final Capstone & Certification

- Hands-on lab integrating all modules
- Realistic malware campaign investigation

- Presentation of findings and attribution evidence
- Panel evaluation and feedback
- Certification exam and course wrap-up
- **Case Study:** End-to-end campaign analysis for certification

Training Methodology

- Instructor-led theory sessions combined with interactive labs
- Real-world case studies with guided threat attribution exercises
- Access to malware sandbox and simulation environments
- Use of industry-grade tools (e.g., Wireshark, Ghidra, MISP)
- Peer collaboration and team-based attribution simulations
- Continuous assessment through quizzes, labs, and final capstone

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

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
10 Aug 2026	21 Aug 2026	Online	$2,200
17 Aug 2026	28 Aug 2026	Online	$2,200
24 Aug 2026	04 Sep 2026	Online	$2,200

Start Date	End Date	Location	Price
31 Aug 2026	11 Sep 2026	Online	$2,200
07 Sep 2026	18 Sep 2026	Online	$2,200
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200
28 Sep 2026	09 Oct 2026	Online	$2,200

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

Register Online Now

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