Training Course on Analyzing IoT Malware and Botnets

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

As the Internet of Things (IoT) ecosystem continues to expand, so too does the threat landscape surrounding it. Malicious actors are increasingly targeting vulnerable IoT devices, transforming them into botnets used for distributed denial-of-service (DDoS) attacks, data breaches, and cyber espionage. Training Course on Analyzing IoT Malware and Botnets is designed to equip cybersecurity professionals, analysts, and researchers with in-depth skills to detect, analyze, and mitigate IoT malware threats using real-world scenarios, automated tools, and forensic methodologies.

Through hands-on labs, reverse engineering exercises, and botnet traffic analysis, participants will explore the anatomy of IoT malware such as Mirai, Hajime, and Mozi. This course emphasizes practical techniques in dynamic malware analysis, network behavior analysis, protocol dissection, and threat intelligence integration, enabling learners to proactively defend IoT environments in industrial, healthcare, and smart home settings.

Programme Curriculum

Training Course on Analyzing IoT Malware and Botnets

Introduction

As the Internet of Things (IoT) ecosystem continues to expand, so too does the threat landscape surrounding it. Malicious actors are increasingly targeting vulnerable IoT devices, transforming them into botnets used for distributed denial-of-service (DDoS) attacks, data breaches, and cyber espionage. Training Course on Analyzing IoT Malware and Botnets is designed to equip cybersecurity professionals, analysts, and researchers with in-depth skills to detect, analyze, and mitigate IoT malware threats using real-world scenarios, automated tools, and forensic methodologies.

Through hands-on labs, reverse engineering exercises, and botnet traffic analysis, participants will explore the anatomy of IoT malware such as Mirai, Hajime, and Mozi. This course emphasizes practical techniques in dynamic malware analysis, network behavior analysis, protocol dissection, and threat intelligence integration, enabling learners to proactively defend

IoT environments in industrial, healthcare, and smart home settings.

Course Objectives

1. Understand the architecture and vulnerabilities of IoT devices
2. Analyze real-world IoT malware strains (Mirai, Mozi, Hajime)
3. Perform network traffic inspection and packet analysis
4. Conduct dynamic and static malware analysis
5. Implement reverse engineering techniques for binary malware
6. Detect and dismantle IoT botnet infrastructures
7. Use honeypots for IoT threat hunting
8. Explore DNS tunneling and C2 communication in botnets
9. Apply machine learning to IoT anomaly detection
10. Correlate threat intelligence with IoT threat patterns
11. Develop automated scripts for malware signature extraction
12. Secure IoT environments through segmentation and authentication
13. Build incident response strategies for IoT botnet attacks

Target Audience

1. Cybersecurity Analysts
2. Network Security Engineers
3. Digital Forensics Experts
4. IoT Device Manufacturers
5. Penetration Testers
6. Malware Researchers
7. SOC (Security Operations Center) Teams
8. Academic Researchers in Cybersecurity

Course Duration: 5 days

Course Modules

Module 1: Introduction to IoT Ecosystem & Security Risks

- Overview of IoT architecture and protocols
- Attack surface in consumer and industrial IoT
- Vulnerability assessment in embedded systems
- Firmware exploitation techniques
- IoT device hardening practices
- **Case Study:** Hacked baby monitors and smart TVs

Module 2: Malware Targeting IoT Devices

- Anatomy of IoT malware
- Static and dynamic analysis of malware samples
- Malware propagation mechanisms in IoT
- C2 communication patterns
- Anti-analysis and obfuscation in IoT malware
- **Case Study:** Deep dive into Mirai botnet evolution

Module 3: IoT Botnet Infrastructure Analysis

- Botnet creation and architecture
- DNS, P2P, and hardcoded C2 channels

- Techniques to intercept botnet traffic
- Role of bulletproof hosting
- IoT botnet takedown strategies
- **Case Study:** Mozi botnet's persistent infections

Module 4: Network Traffic and Packet Analysis

- Capturing traffic using Wireshark and Tshark
- Identifying IoT protocols (MQTT, CoAP, UPnP)
- Signature-based and anomaly-based detection
- DDoS traffic fingerprinting
- Automated log analysis using ELK stack
- **Case Study:** Botnet-based DDoS attack on Dyn

Module 5: Malware Reverse Engineering for IoT

- Reverse engineering ARM/MIPS binaries
- IDA Pro and Ghidra for embedded systems
- Identifying hardcoded credentials and backdoors
- Extracting indicators of compromise (IOCs)
- Analyzing shell scripts used in malware deployment
- **Case Study:** Reverse engineering the Hajime worm

Module 6: IoT Threat Hunting Using Honeypots

- Setting up IoT honeypots (Honeyd, Cowrie)
- Logging and analyzing attacker behavior
- Attracting and sandboxing malware samples
- Visualizing threat data
- Integrating honeypot data with SIEM systems
- **Case Study:** Real-world attack logs from Telnet honeypots

Module 7: Machine Learning for IoT Malware Detection

- Supervised vs unsupervised detection models
- Feature engineering from network logs
- Dataset preparation and labeling challenges
- Using scikit-learn and TensorFlow for IoT data
- Model evaluation and deployment
- **Case Study:** ML model detecting botnet behavior

Module 8: Building a Response Strategy to IoT Botnet Attacks

- Incident response lifecycle for IoT malware
- Communication plans and forensic readiness
- Restoring services post-botnet attack
- Legal and regulatory compliance (GDPR, NIST, etc.)
- Coordinating with ISPs and CERTs
- **Case Study:** Nation-state attack exploiting IoT webcams

Training Methodology

- Hands-on labs using real IoT malware samples
- Simulated attack and defense scenarios
- Guided walkthroughs of malware and botnet analysis
- Use of industry-standard tools (Wireshark, Ghidra, ELK, Cowrie)

- Group discussions on case studies and emerging threats
- Knowledge checks and practical assessments

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	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 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