# Real Time College

## Course: Malware Analysis

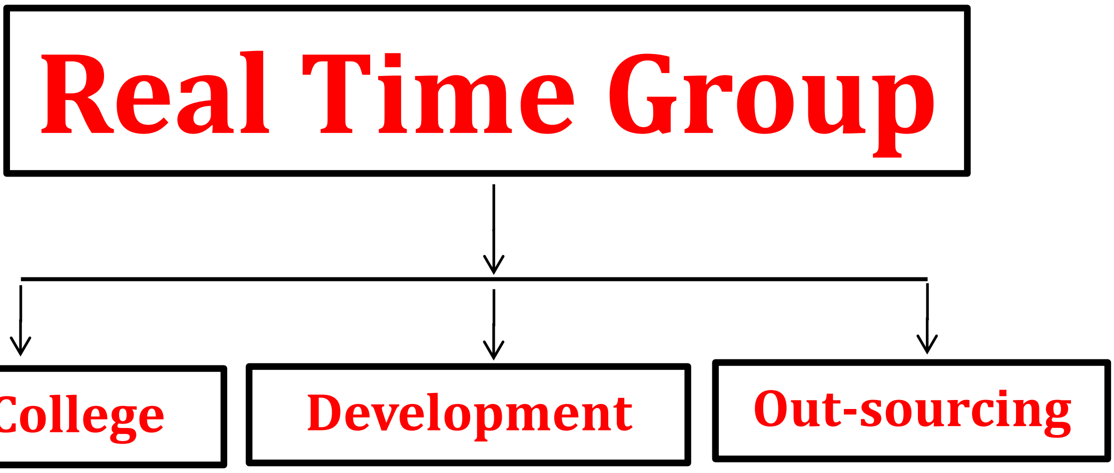
**Duration:** 40 Hours

Hands-On-Training: 50%

Real Time Group is a multi-disciplinary dynamic and innovative Real-Time O.S. and Software Solutions Center, established in 2007.

Providing Software, Security and Embedded Linux solutions, professional services and consulting, end-to-end flexible system infrastructure, outsourcing, integration and training services for Hardware, Software and RT-OS \ Embedded Systems.

The company is divided into the following three Divisions:



Real Time Group

College

Development

Out-sourcing

rt-ed.co.il

rt-dev.com

rt-hr.co.il

## Training Division:

Professional Training Services for Software, Cyber Security, IT, RT-OS and Embedded systems industries.

We provide the knowledge and experience needed to enable professional engineers to Develop, Integrate and Automate Hardware, Software and Networking Projects.

To ensure experience, all courses are practical – Hands-On-Training.

The latest Development, Cyber Security, IT and Automation equipment which are adopted by the industry are used.

All students are supplied with necessary equipment (i.e. software license, AWS Account, etc ) for Class -work \ Home-work and course projects.

## Course Overview:

This **Malware Analysis Course** is part of RT-Group's Cyber-Security Complete Track hand-on-training course, which provides the most complete and comprehensive Cyber Security Course.

Malware analysis is very important for Cyber security, its used by analysts to create IOC's. Malware may come in many forms, such as: viruses, spyware, worms, Trojan horses. Their functionalities might be different, but they all aim to gather information about the infected device \ user without his knowledge, or authorization.

During the course we'll target all Malware hazards including Malware Static and Dynamic Analysis Techniques.

By the end of the course you'll know how to handle Malware Analysis Techniques, Assembly Fundamentals, Reverse Basics, Reversing RATs and Keylogger files, Memory Analysis, Windows Internals, Dynamic Malware Analysis Techniques, Static Malware Analysis Techniques, Malicious Document Analysis and Reverse engineering concepts.

Workshops comprise approximately 50% of class time and are based around carefully designed exercises to reinforce and challenge the extent of learning.

## Who should attend:

- Student with no experience who wish to learn Cyber Security – **must first pass the Cyber Fundamentals Exam\Course**.
- Candidates seeking to join **SOC teams** and specialize in forensics and cyber incident investigation.
- System\Linux Administrators wishing to upgrade their skills in Cyber Security.
- Architects \ Team Leaders \ Engineers \ Programmers who wish to participate in Cyber Security projects.

## Prerequisite:

- A basic level of computer literacy is expected, using a PC running Windows.
- You should have a basic understanding of networking concepts.
- No previous experience in cyber security is necessary

# Malware Analysis

1. **Introduction to Malware**
   a. What is Malware?
   b. Malware types.
   c. Viruses, spyware, worms, Trojan horses, Rootkits, Backdoors and more.
   d. What's common to all Malware types ?

2. **Vulnerability**
   a. Security defects in software
   b. Insecure design or user error
   c. Over-privileged users and over-privileged code
   d. Operating Systems API's

3. **Malware Detection**
   a. Detecting Unknown Threats
   b. Identifying Related Threats
   c. Malware Detection
   d. Malware Use Cases
   e. Fully automated analysis:

4. **Malware Analysis Techniques**
   a. Static properties analysis
   b. Dynamic Malware
   c. Interactive behavior analysis
   d. Manual code reversing.
   e. Memory Analysis