


# **THE HIGHEST QUALITY CYBER SECURITY TRAINING**

We believe your cyber security team deserves a better learning experience





Our instructors and mentors are recognized throughout the cybersecurity world as the world's best operators and reverse engineers. Their specializations vary from mobile malware research, to reverse engineering, to technology development. Routinely, our teachers are invited to participate in international events and are a sought after voice in shaping policies and defensive strategies to contest Advanced Persistent Threat presence on friendly networks around the globe.

Our mentors have built and delivered many courses in computer science, information technology and engineering up to and including the university level. They take it as their personal mission to build upon and disseminate Arc4dia's technical expertise, in order to help businesses to protect and defend themselves from cyber threats.

## Why choose ARC4DEMY?

Experienced instructors - thousands of hours of operational experience in each subject area

Courses tailored to any student level - basic lab exercises building to force-on-force scenarios

Exclusive content - access to knowledge and skills rarely taught in schools and universities

Cutting-edge tools and techniques - exposure to advanced and complex tools and tradecraft

## THE RESULT

True operational knowledge transfer enhancing your team's tactical advantage.



## ABOUT ARC4DIA

A privately held company, ARC4DIA Cyber Defense has been an industry leader in the cyber security industry since its inception in 2010. Creators of SNOW, the world's most comprehensive cyber defence platform, the company protects more than \$40 billion dollars in assets globally, including government agencies along with mid to large scale enterprises across a variety of sectors.

With more than 60 years of combined counter-APT operations experience, the ARC4DIA team is a group of highly-skilled cyber experts hand-picked from the military, national security agencies, government, and academic institutions around the world.





# THREAT DETECTION AND SIMULATED ENGAGEMENT



5 days



## Course Overview

Introduction of malware detection through its behaviours, storage and persistence tricks.

The first part of the course covers how to use Windows system introspection tools to find occurrences of running malware. While using Arc4dia's SNOW technology, the second part involves hands-on detection of malware and attacks live across a lab infrastructure.

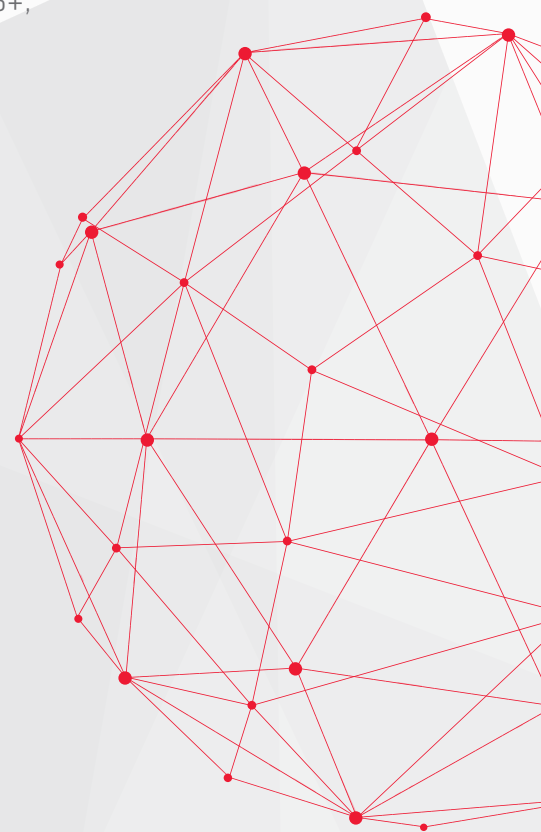
## Materials to bring +

Laptop computer able to run 64-bits virtual machines.

VMware Workstation 11+, or VMware Fusion 6+, or VMware Player 11+

## Course prerequisites

Intro to Reverse Engineering







## Course Breakdown

### Day 1

Dynamic malware hunting

- Hunting with Sysinternals tools
- Thread injection
- Hiding modules
- Autoruns
- API hooking

### Day 2

Malware appearance and behaviour

- False positives and false negatives
- Destructive malwares
- Rootkits

### Day 3

Forensic analysis

- Volatility framework
- System dumping
- Process hiding
- Code injection
- Process dumping
- Footprints


### Day 4

Hunting with SnowBoard 1

- Introduction to Snow
- Introduction to the SnowBoard interface
- Alert investigation
- Statistic investigation

### Day 5

Hunting with SnowBoard 2

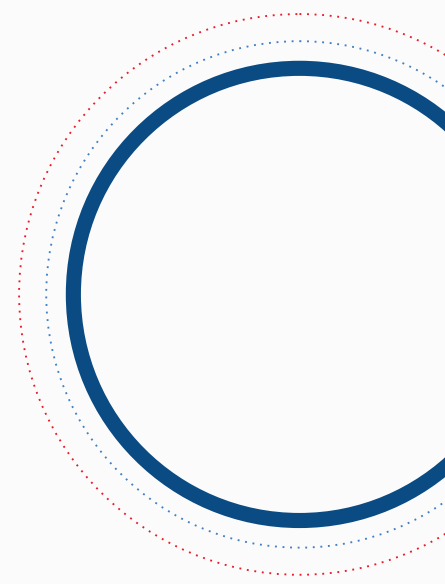
- Clustering rules
  - Cloud modules
  - Malware profiles
- 



# WEB SECURITY



2 days



## Course Overview

While using hands-on labs, this short course presents the most common security vulnerabilities that plague web sites and applications, and how to exploit these vulnerabilities in order to better defend against them.

Topics covered include command injection, file upload and inclusion, SQL injection, cross-site scripting (both reflected and stored) and cross-site request forgery.

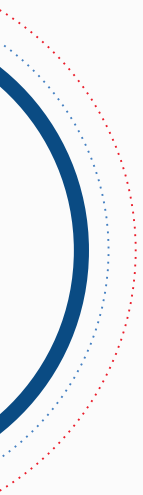
## Materials to bring +

Laptop computer able to run 64-bits virtual machines.

VMware Workstation 11+, or VMware Fusion 6+, or VMware Player 11+

## Course prerequisites

Medium-level web technology knowledge: HTML 5, Javascript, PHP, relational databases



## Course Breakdown

### Day 1 Server-side attacks

- Command injection
- File inclusion
- File upload
- SQL injection

### Day 2 Client-side attacks

- Reflected cross-site scripting
- Stored cross-site scripting
- Cross-site request forgery
- Enhancing the defensive posture





**ARCADIA**  
Cyber defense

# ADVANCED REVERSE ENGINEERING



5 days



## Course Overview




This course follows up on the introduction and completes the budding reverse engineering skills of students against modern, APT-related malware.

We start by discussing how malware conceals its behaviour to prevent reverse engineering including the following: encryption, compression, mangling and self-unpacking shims.

We then present how malware hides itself to persist on a system, either as a user-mode program, or as a kernel-mode module.

Other covered subjects include communication features for communicating with other processes, command and control infrastructure, malware implemented using exotic runtime technologies, and signature malware behaviour, such as keylogging and privilege elevation.



## Materials to bring +

Laptop computer able to run 64-bits virtual machines.

VMware Workstation 11+, or VMware Fusion 6+, or VMware Player 11+

## Course prerequisites

Intro to Reverse Engineering





## Course Breakdown

### Day 1

APTs and their configurations

- Mangling
- Compression
- Encryption
- Self-unpacking

### Day 2

Malware hiding techniques

- Code injection
- API hooking
- Hook injection
- APC injection
- Process hollowing
- SSDT hooking
- Filter drivers

### Day 3

Malware communication

- Inter-process communication
- Configuration files
- File transfer
- C2 communication

### Day 4

Strangely constructed malware

- C++
- COM
- Delphi

### Day 5

Recognizing typical constructs

- Key logging
  - Shell redirection
  - Privilege escalation
  - Driver/service installation
- 

**ARCADIA**

Cyber defense



# APT TACTICS AND DEFENSE



3 days



## Course Overview

In this short course, we aim to present how malware relates to APTs and how they differ from that used in more common, untargeted attacks.

We detail the typical intentions of an attacker and the tools and processes they would leverage to attain these goals.

Lastly, the course presents key approaches to detect and terminate the process of an APT, and the infrastructure required for effective incident response.

## Materials to bring +

Laptop computer able to run 64-bits virtual machines.

VMware Workstation 11+, or VMware Fusion 6+, or VMware Player 11+

## Course prerequisites

None



## Course Breakdown

### Day 1 Targeted attacks: why and how

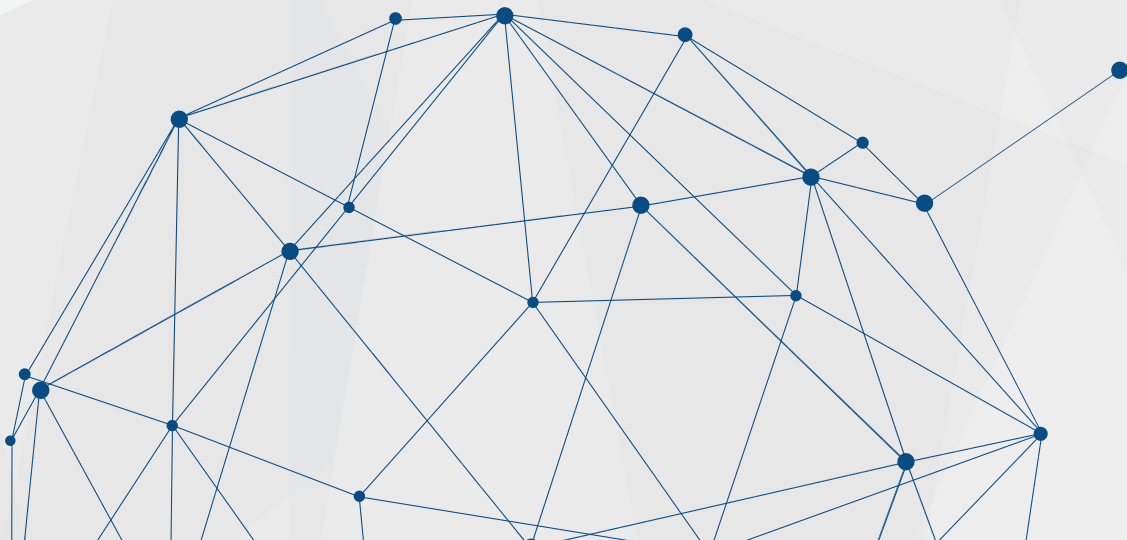
- Goals of the APT
- Software attacks
- Non-software attacks
- People-based attacks

### Day 2 Tactics and footprint of targeted attacks

- Defense systems and their weaknesses
- Signs of attacks

### Day 3 Effective defense against targeted attacks

- Pitfalls of attribution and deniability
- Reverse engineering
- Undermining exploitation
- CERT team cooperation and sharing





**ARCADIA**  
Cyber defense

# **INTRODUCTION TO REVERSE ENGINEERING**



**5 days**



## Course Overview

In this course we present the fundamental skills for understanding the malware actions and behaviour of Windows programs.

We start with an introduction to Intel assembly language - both 32 and 64 bit, and carry on with a detailed exposition of Windows executables and dynamic libraries. Reverse engineering of actual malware examples are then presented in a tutorial fashion using professional disassembly and debugging software.

Through hands-on labs, the students learn how to defeat code obfuscation and techniques used by malware authors to hamper dynamic reverse engineering.

### Materials to bring +

Laptop computer able to run 64-bits virtual machines.

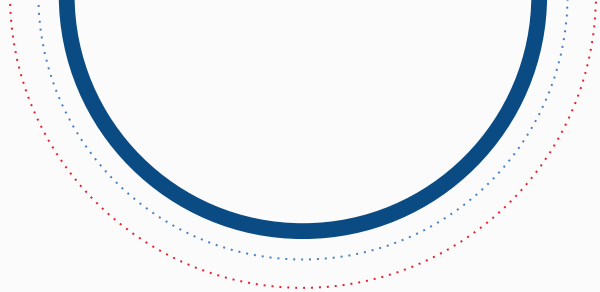
VMware Workstation 11+, or VMware Fusion 6+, or VMware Player 11+

### Course prerequisites

Medium-level computer programming skills







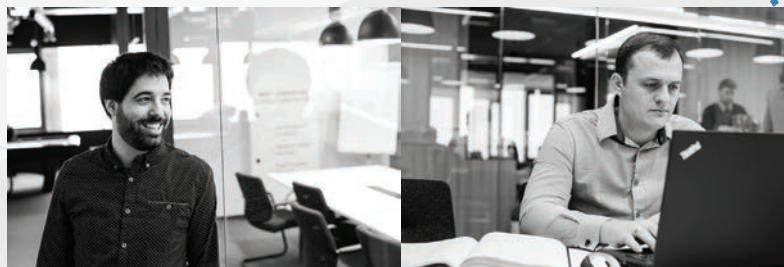
## Course Breakdown


- Day 1** Static reverse engineering
- Introduction
  - Binary analysis
  - PE file format
  - Introduction to x86 assembly
  - Introduction to IDA
- Day 2** Dynamic reverse engineering
- VM configuration
  - Sysinternals tools for reverse engineering
  - Introduction to the IDA debugger
- Day 3** Common malware behaviours
- Types and families
  - Persistence
  - Data encoding
- Day 4** Advanced dynamic reverse engineering
- Introduction to AMD64
  - Code obfuscation
  - Real malware reverse engineering
- Day 5** Anti-reverse engineering techniques
- Basic techniques
  - Bypass approaches



## Teachers at ARC4DEMY

Our teachers are recognized throughout the cybersecurity community as some of the world's best reverse engineers, who share their talents and experience throughout the trainings. Their specialization varies from mobile malware research, reverse engineering up to technology development. Routinely, our teachers are invited to participate in international events and be a sought after voice in shaping policies and defensive strategies to contest Advanced Persistent Threat presence on friendly networks around the globe. Our mentors have built and taught multiple courses in computer science, information technology and engineering. They take it as their personal mission to build upon and disseminate Arcadia's technical expertise, in order to help businesses to protect and defend themselves from cyber threats.





**PARTNER WITH US,**  
seize the initiative,  
take the fight  
to the adversary.

**Montreal | London | vilnius**  
**info@arc4dia.com**  
**www.arc4dia.com**