Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

Malware Lifecycle - from offensive to defensive

CODE:	LENGTH:	PRICE:
OTH_MLC	16 Hours (2 days)	€1,300.00

Description

This workshop is focusing on offensive nature in cyber security trough malware usage. It is leading out the attendances from the classical definitions and appearance of malware to new world of malware that progress through combined techniques and adopting hybrid attacks. The content is designed to be simple and meaningful with hands on experience. The focus will be on malware designed for attacking Microsoft Windows platforms.
Duration 2 days (09h-16h) 90 minutes coffe and lunch break time

Prerequisites

Instruction for LABs
The workshop is BYOD so the attendances must have their own laptop with 90GB free space, 8GB RAM and processor that support virtualization. They will be instructed to install VMware workstation at the beginning of the course and after they will receive USB memory device to copy the VMs locally. (This can go also with online labs)

Programme

Section 1 - Fundamentals of Malware
Starting from very short history look on malware followed by categorized view of families and stages of malware, the attendances can see the whole picture of one malware.
Section 2 - Malware techniques
With various malware techniques that appear trough history, we witness utilizing technology, weaknesses and vulnerabilities to achieve success in the hacking attack. They will be covered in this section with practical examples that can make attendances experience real life malware attacks.
Section 3 - Building malware
Since the theory is nothing without practice, this section has the goal to give the attendances opportunity to build the malware all by themselves and test it in controlled sandbox environment.
Section 4 - Malware analysis
Here we will learn what can we do to find indications of malware activity and decode the nature of its intent. Will be showing opportunities for online sandboxing that can speed up the analysis and save meaningful time.

Session Dates

Aikataulutamme kiinnostuksen mukaan.

Additional Information

This training is also available as onsite training. Please contact us to find out more.