Office Document Analysis

We propose a two-day training named «Office documents analysis».
It will enable you to understand how the malwares are using office documents as initial infection stage.
It will help your Incident response team to determine by itself if an office document is malicious.
At the end of the training, you will be able to extract the payload and determine the IOC of a sample.
The training is 50% lectures and 50% lab.

The course will start by a refresh on the current threat landscape. The student will learn how to setup his own office analysis lab and will learn and practise the identification, analyse on various malicious office documents.
The student will learn how obfuscation is in place and how to isolate a shellcode or an malicious payload.
After this formation, the student will be able to qualify the maliciousness of a given office document by his own.

Détails

- Code : ISMS-Office
- Durée : 2 jours (14 heures)

Public

- Developers
- System administrators
- Systems engineers

Pré-requis

- Knowledge of Linux, Python and scripting

Objectifs

Programme

The following courses syllabus will be learned :

- Treat landscape
- Setup forensic Lab and Tools
- Why opening theses files & document identification
- Understand how macro deliver payload
- Extraction of Macro
- Macro Goal
- Obfuscation

Modalités

- Type d’action :Acquisition des connaissances
- Moyens de la formation :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- Modalités pédagogiques :Exposés – Cas pratiques – Synthèse
- Validation :Exercices de validation – Attestation de stages