

## FORMATION

○ **TITRE : Outils et techniques d'analyse de code malveillant**

○ **OBJECTIFS PÉDAGOGIQUES**

- Apporter les connaissances fondamentales afin d'analyser les programmes malveillants,
- Utilisation des outils tel que des désassembleurs, des débogueurs et d'autres outils afin d'analyser leur comportement dans un environnement maîtrisé et sécurisé.

○ **DESCRIPTIF DU COURS**

L'objectif de la formation est d'apporter les connaissances fondamentales afin d'analyser les programmes malveillants en utilisant des outils tel que des désassembleurs, des débogueurs et d'autres outils afin d'analyser leur comportement dans un environnement maîtrisé et sécurisé.

**(Voir programme du cours en page 2)**

## MODALITÉS PRATIQUES

○ **DURÉE/NOMBRE D'HEURES**

5 jours / 30 heures

Prochaine session : 8, 9, 10, 29 et 30 nov. 2021

○ **PRÉREQUIS D'ACCÈS À LA FORMATION**

- Connaissances de base sur les systèmes d'exploitation,
- Connaissances élémentaires en langage Python (boucles, listes, ensemble, chaînes de caractères) et de bash/console.

○ **ÉQUIPEMENT NÉCESSAIRE**

Ordinateur portable disposant des éléments suivants :

- Système d'exploitation à jour (Windows XP, 7 ou 8)
- RAM : 4 Go minimum
- WiFi
- VMWare

○ **LIEU DE FORMATION**

Mines Nancy, campus Artem

○ **TARIFS :**

2 750 € net par personne, déjeuner compris

## CONTACT

○ **RESPONSABLE PÉDAGOGIQUE**

Guillaume BONFANTE

✉ guillaume.bonfante@mines-nancy.univ-lorraine.fr  
Tél : +33 3 72 74 49 58

○ **CONTACT ADMINISTRATIF**

Mines Nancy

Service de la DFSC

✉ mines-nancy-dfsc@univ-lorraine.fr  
Tél : +33 3 72 74 48 67

## PLAN DU COURS

### ○ **MODULE 1 : INTRODUCTION**

#### **À L'ANALYSE DE CODE MALVEILLANT**

Ce module est destiné à présenter les connaissances fondamentales nécessaires à l'analyse de codes malveillants en laboratoire. Il couvre notamment les aspects comme la configuration et l'architecture d'un laboratoire de haute sécurité.

### ○ **MODULE 5**

#### **MÉCANISMES DE PROTECTION DE MALWARES**

Présentation générale des techniques de protection de code : Méthode d'anti-virtualisation, anti-débogage, Offuscation par rajout de code mort, Chiffrement de code par opérations arithmétiques, Auto-modification de code.

### ○ **MODULE 2/3**

#### **SCÉNARIOS D'ATTAQUE PAR MALWARE**

Nous reproduisons deux schémas typiques et réels d'attaque de malware. Pour les deux, nous décrivons les principes d'une organisation mafieuse : le rôle de chacun, leur intérêt, et l'utilisation de techniques afférentes.

### ○ **MODULE 6/7**

#### **ANALYSE AVANCÉE**

Présentation de PIN et des Pintool, Conception et analyse de traces d'exécution, Visualisation de l'automodification, Contre-mesures anti-anti-débogage et anti-anti-virtualisation, Suivi de processus, Pilotage d'une machine virtuelle dédiée à l'analyse.

### ○ **MODULE 4**

#### **ANALYSE DE CODE MALVEILLANTS**

Rappels sur le code assembleur, Rappels sur les aspects systèmes, chargement d'un PE en mémoire, clés de registre, driver, DLL, Analyse d'un malware : présentation d'une technique de chiffrement.

### ○ **MODULE 8**

#### **DOCUMENTS MALVEILLANTS,**

#### **ANALYSE DE LA MÉMOIRE**

Ce module permet de comprendre comment analyser les documents Office et PDF pouvant contenir une payload. Présentation d'exploits, metasploit, Recherche en mémoire d'indices d'infections, Extraction de code.

### ○ **MODULE 9/10 : EXERCICE FINAL**

Application des connaissances à travers un exercice pratique concret. Nous demandons aux étudiants d'analyser un malware que nous avons reconstitué à partir de codes existants, typiquement Duqu, Zeus, Regin. Le travail est réalisé par groupe de deux étudiants.