Outils et techniques d'analyse de code malveillant

FORMATION

- **Titre : Outils et techniques d'analyse de code malveillant**

- **École :** Mines Nancy

- **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 plan du cours en page 2)

MODALITÉS PRATIQUES

- **Durée/nombre d'heures :**
  5 jours / 30 heures

- **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

- **Tarifs :**
  2750 € net par personne, déjeuner compris

CONTACT

- **Responsable pédagogique**
  Guillaume BONFANTE
  guillaume.bonfante@univ-lorraine.fr

- **Contact administratif**

  Mines Nancy
  Service de la DFSC
  mines-nancy-dfsc@univ-lorraine.fr
  Tél : +33 3 55 66 26 82

MINESnancy
ARTEM

Outils et techniques d'analyse de code malveillant

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 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 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 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 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-debogage et anti-anti-virtualisation, Suivi de processus, Pilotage d'une machine virtuelle dédiée à l'analyse

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.