

RÉTRO-INGÉNIERIE DE LOGICIELS MALVEILLANTS

Créez votre laboratoire d'analyse de malwares et comprenez leur fonctionnement en plongeant dans leur code.

Cette formation prépare à la réalisation d'investigations dans le cadre d'attaques réalisées via des logiciels malveillants, de la mise en place d'un laboratoire d'analyse comportementale à l'extraction et au désassemblage de code malveillant.

Code : RILM

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.

JOUR 1

Rappels sur les bonnes pratiques d'investigation numérique

Présentation des différentes familles de malwares

Vecteurs d'infection

Mécanisme de persistance et de propagation

Laboratoire virtuel vs. physique

- Avantages de la virtualisation
- Solutions de virtualisation

Surveillance de l'activité d'une machine

- Réseau
- Système de fichiers
- Registre
- Service

Ségrégation des réseaux

- Réseaux virtuels et réseaux partagés
- Confinement des machines virtuelles
- Précautions et bonnes pratiques

Variété des systèmes

Services usuels

- Partage de fichiers
- Services IRC (C&C)

Licensing

- Importance des licences

JOUR 2

Mise en place d'un écosystème d'analyse comportementale

- Configuration de l'écosystème
- Définition des configurations types
- Virtualisation des machines invitées
 - VmWare ESXi
 - Virtualbox Server

Installation de Cuckoo/Virtualbox

Mise en pratique

- Soumission d'un malware
- Déroulement de l'analyse
- Analyse des résultats et mise en forme

Amélioration via API

- Possibilités de développement et améliorations

JOUR 3

Analyse statique de logiciels malveillants

- Prérequis
 - Assembleur
 - Architecture
 - Mécanismes anti-analyse
- Outils d'investigation
 - IDA Pro
- Utilisation d'IDA Pro
 - Méthodologie
 - Analyse statique de code
 - Analyse de flux d'exécution
- Mécanismes d'anti-analyse
 - Packing/protection (chiffrement de code/imports, anti-désassemblage)

- Machine virtuelle
- Chiffrement de données
- Travaux pratiques
 - Analyse statique de différents malwares

JOUR 4

Analyse dynamique de logiciels malveillants

- Précautions
 - Intervention en machine virtuelle
 - Configuration réseau
- Outils d'analyse
 - OllyDbg
 - ImmunityDebugger
 - Zim
- Analyse sous débogueur
 - Step into/Step over
 - Points d'arrêts logiciels et matériels
 - Fonctions systèmes à surveiller
 - Génération pseudo-aléatoire de noms de domaines (C&C)
 - Bonnes pratiques d'analyse
- Mécanismes d'anti-analyse
 - Détection de débogueur
 - Détection d'outils de rétro-ingénierie
 - Exploitation de failles système

Suite...

PROGRAMME

JOUR 5

Analyse de documents malveillants

- Fichiers PDFs
 - Introduction au format PDF
 - Spécificités
 - Intégration de JavaScript et possibilités
 - Exemples de PDFs malveillants
 - Outils d'analyse: Origami, Editeur hexadécimal
 - Extraction de charge
 - Analyse de charge

- Fichiers Office (DOC)
 - Introduction au format DOC/DOCX
 - Spécificités
 - Macros
 - Objets Linking and Embedding (OLE)
 - Outils d'analyse: Oledump, Editeur hexadécimal
 - Extraction de code malveillant
 - Analyse de la charge

- Fichiers HTML malveillants
 - Introduction au format HTML
 - Code JavaScript intégré
 - Identification de code JavaScript malveillant
 - Outils d'analyse: éditeur de texte
 - Désobfuscation de code
 - Analyse de charge

PROCHAINES DATES

14 mars 2022,
30 mai 2022,
26 sept. 2022



OBJECTIFS

- Mettre en place un laboratoire d'analyse de logiciels malveillants
- Savoir étudier le comportement de logiciels malveillants
- Analyser et comprendre le fonctionnement de logiciels malveillants
- Détecter et contourner les techniques d'autoprotection
- Analyser des documents malveillants



INFORMATIONS GÉNÉRALES

Code : RILM

Durée : 5 jours

Prix : 3 500 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois-Perret (92)



PUBLIC VISÉ

- Techniciens réponse aux incidents
- Analystes techniques
- Experts sécurité



PRÉ-REQUIS

- Connaissance du système Microsoft Windows
- Maîtrise du langage assembleur 32 et 64 bits
- Maîtrise de l'architecture 32 et 64 bits Intel



RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne / Internet