Rétro-Ingénierie des Logiciels Malveillants

Introduction

- Rappels sur les bonnes pratiques d'investigation numérique
- Présentation des différentes familles de malwares
- Vecteurs d'infection
- Mécanismes de persistance et de propagation

Laboratoire d'Analyse

- Laboratoire virtuel vs. physique
  - Avantages de la virtualisation
  - Solutions de virtualisation
- Ségrégation des réseaux
  - Réseaux virtuels et réseaux partagés
  - Confinement des machines virtuelles
  - Précautions et bonnes pratiques

Supervision de l'Activité d'une Machine

- Réseau
- Système de fichiers
- Registre
- Services

Initiation à l'Analyse Comportementale

- Variété des systèmes

Mise en Place d'un Écosystème d'Analyse Comportementale

- Configuration de l'écosystème
- Définition des configurations types
- Virtualisation des machines invitées
  - VMware
  - VirtualBox
- Installation de CAPEv2 et 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 d'améliorations

Analyse Dynamique de Logiciels Malveillants

- Précautions
  - Intervention en machine virtuelle
  - Configuration réseau
- Outils d'analyse
  - OllyDbg
  - Immunity Debugger
- Analyse sous débogueur
  - Step into / Step over
  - Points d'arrêt 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

Analyse de Documents Malveillants

- Fichiers PDF
  - Introduction au format PDF
  - Spécificités
  - Intégration de JavaScript et possibilités
  - Exemples de PDF malveillants
  - Outils d'analyse : OLE Tools, éditeur hexadécimal
  - Extraction et analyse de la charge
- Fichiers Office (DOC/DOCX)
  - Introduction aux formats DOC/DOCX
  - Spécificités
  - Macros
  - Objets Linking and Embedding (OLE)
  - Outils d'analyse : OLE Tools, éditeur hexadécimal
  - Extraction de code malveillant et analyse
- Fichiers APK
  - Introduction au format APK
  - Outils d'analyse : jadx, Frida, Genymotion, MobSF
  - Contournement des protections d'émulation
  - Compréhension du fonctionnement des applications

Découvrez aussi nos autres formations en cybersécurité et en informatique :

- Formation Cybersécurité – Sécurité informatique
- Formation Ethical Hacking et Tests d'intrusion
- Toutes nos formations en informatique

Pour en savoir plus sur la rétro-ingénierie, consultez la ressource suivante :

[Qu’est-ce que la rétro-ingénierie ? — Wikipédia]

Nous contacter:
Doussou Formation
Email: info@doussou-formation.com
http://doussou-formation.com