Introduction à l'analyse de logiciels malveillants

UQAM 2020 - shorturl.at/dtPX6

$ whoami

- Code Reverser chez Google pour Safe Browsing
  - 1.5 ans
- Ex-directeur de PolyHack puis PolyHx - Branche sécu (Polytechnique)
  - 3.5 ans

$ whatis malware

- Un programme agissant contre l'intérêt de l'utilisateur
- Plusieurs formes:
  - Ransomware
  - Infostealer
  - Botnet
  - Backdoor
  - Trojan
  - Cryptominer
  - Adware
  - Etc.
- De plus en plus organisés
- Pour faire de l'argent, pour obtenir des informations, pour manipuler des engagements sur les réseaux sociaux, etc.

Environnement pour analyser du malware

- VM Windows / machine dédié
  - Infecter son poste de travail est rarement une bonne idée
- Outils (voir diapos suivantes)
- Pour les exercices: sans Internet
- Dans la vraie vie: probablement besoin d'Internet pour faire quelque chose d'intéressant

“Reversing mindset”

- Répondre à une question
  - “Est-ce malveillant?”
  - “Comment est-ce que ce programme communique avec son serveur?”
  - “Comment ce programme obtient de la `persistance`?”
  - “Comment est-ce distribué?”
  - Concentre les efforts
- Quels sont les infos facile à trouver?
  - Strings
  - Imports, exports
  - Quelle librairie est utilisé?
  - Que ce passe-t-il sur le réseau?

RPISEC Malware Course

- https://github.com/rpisec/malware
- Chaque lab a un ZIP avec le mot de passe “infected”
- Basé sur un excellent livre pour débuter: Practical Malware Analysis
- Slides + labs + solutions
- Vous permet de continuer

Reconnaissance

- VirusTotal.com
  - PowerShell Get-FileHash | sha256sum
- Articles de blog technique
  - Malpedia, Welivesecurity, SecureList, Blogs independants
  - Eviter tout ce qui est “knowledge base”, “how to remove”, forums de support technique
- Environnements de tests dynamique public
  - any.run, CAPE

Analyse statique de base

- strings!
- Imports/Exports
- Entropie
- Hexdump
- Packing
  - DetectItEasy
  - UPX
  - Dumping manuel

Analyse dynamique de base

- Sysinternals Suite
  - Surtout Process Monitor, Process Explorer
- WireShark/Burp/Fiddler/MITMProxy
  - Regarder le trafic réseau, intercepter les requêtes, même HTTPS

Analyse statique modérée

- Ghidra, IDA Pro, Binary Ninja, JEB, Hopper
  - Désassemble et décompile un exécutable
  - Regarder les différentes fonctions
  - les appels d'API et comment ils se succèdent
  - Interactif: renommer TOUT
  - Imports/exports
  - Scriptage

Analyse dynamique modérée

- Débogueurs
  - x64dbg, windbg, ollydbg
  - Breakpoints, extraire la mémoire (mem dump), regarder les paramètres des fonctions
- Ré-implémentation du protocole réseau
  - Permet d'avoir des informations directement du serveur de commande et contrôle (C2/CnC)

Démo - Lab01-1

github.com/rpisec/malware

pass: infected

Lab01-3

Opportunités à Montréal

- Stages chez
  - Google: https://g.co/kgs/GK3BF5 et hugen@google.com
  - ESET: écrire à dorais@eset.com
  - GoSecure: gosecure.net
  - PNF Software: pnfsoftware.com ou venir me parler

Entrevues chez Google

Stages

- 2 x entrevues par Hangouts (vidéoconférence)
  - 1 technique, 1 RH

Emplois

- 2 x entrevues par Hangouts
- 4 x entrevues en personne

Trucs pour entrevue

- TOUT dire ce que vous pensez
  - Le pire c'est un 5 minutes de silence
  - Votre interviewer peut vous clarifier des choses, vous ré-enligner
- Commencer par une solution naïve puis itérer
- Cherchez des exemples en ligne (surtout YouTube)
- Pratiquez à coder sur un tableau
  - De plus en plus sur Docs mais pas encore à 100%
- Prenez le langage où vous êtes le plus à l'aise
- Posez des questions
- Clarifiez les instructions
- Testez votre code/solution

Communauté Montréalaise de Sécurité Informatique

- Clubs universitaires:
  - PolyHx, DCIÉTS, UQAM-AGEEI, etc.
- Montréhack.ca - Ce soir!
- Nsec.io
- Hackfest.ca