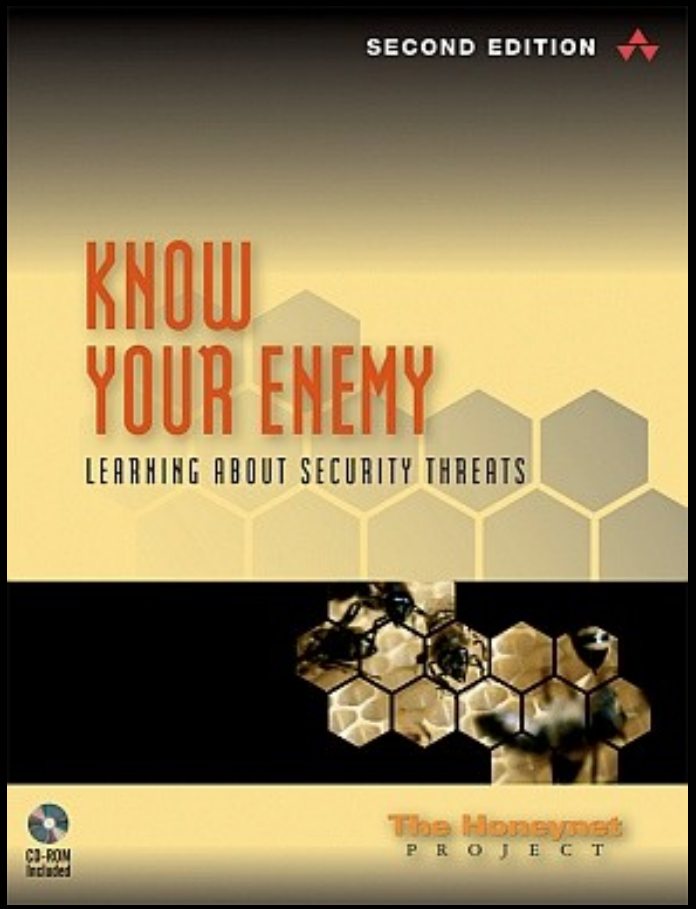
THE HONEYNET PROJECT

The Honeynet Project, Google et vous...

THE HONEYNET PROJECT



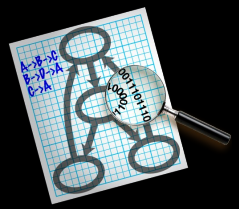
- Communauté de chercheurs en sécurité fondée en 1999 par Lance Spitzner
- Objectifs :
  - Comprendre les techniques utilisées par les attaquants
  - Développer et mettre à disposition des outils de détection (honeypots) et d'analyse
- Coopération avec d'autres organisations :
  - Conficker Working Group
  - ShadowServer
  - Google (GSoC)
- http://honeynet.org/

- Google Summer of Code est un programme lancé en 2005 par Google dont l'objectif est de rémunérer des étudiants qui développent ou aident à développer des logiciels Open Source.
- Depuis son lancement : 4.500 étudiants, 300 projets Open Source
- Principe :
  - Un tuteur : propose une idée
  - Un ou plusieurs étudiants qui développent cette idée
- En 2011 :
  - 175 organisations : Apache, CERN, Debian, FreeBSD,GNU, The Honeynet Project
- 988 projets acceptés
- 5500 USD
  - 5000 pour le développeur
  - 500 pour le tuteur (ou l'organisation)
  - http://www.google-melange.com/gsoc/projects/list/google/gsoc2011

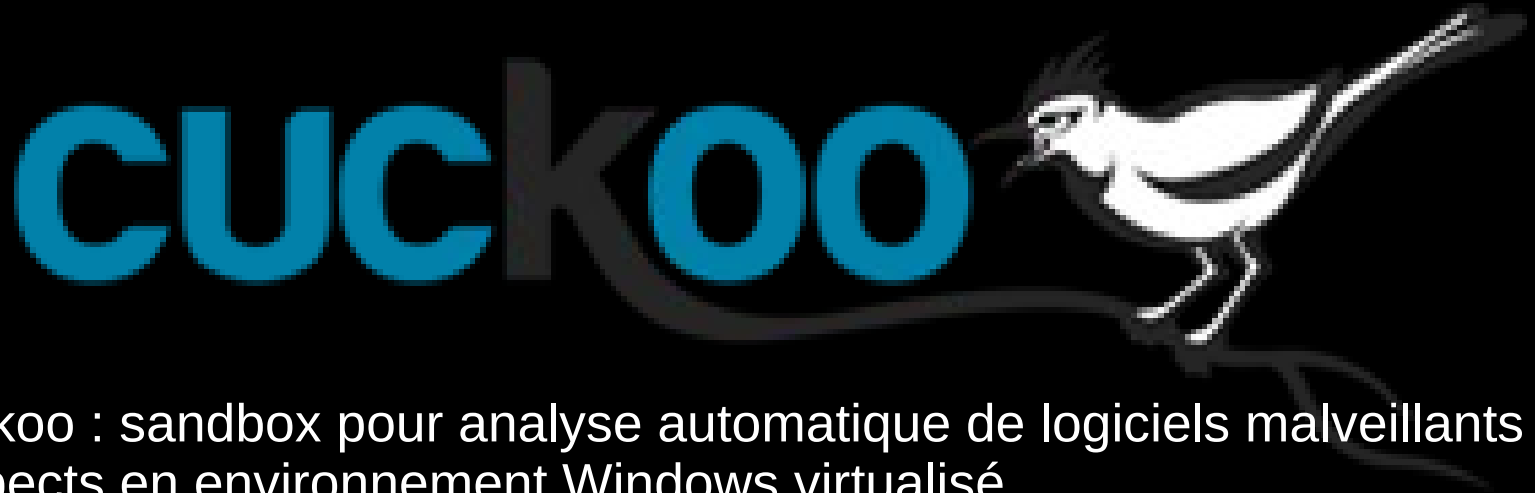
THE HONEYNET PROJECT

- 12 projets de développement tutorés :
  - Improve our high interaction client honeypot Capture-HPC
  - HonEeeBox Data Management Interface
  - Honeynet Visualization
  - Web based visualization for malware/attack analysis
  - DroidBox: An Android Application Sandbox for Dynamic Analysis
  - Static Analysis of Android Malware
  - Network Sinkhole
  - ***Extending Wireshark Analysis***
  - ***Cuckoobox***
  - Hypervisor data collection
  - VoIP low interaction server honeypots
  - Improving shellcode emulation performance

Extending Wireshark Analysis



- Développer des patch dans le but d'étendre les capacités de Wireshark (branche 1.7 Development) dans un contexte « inforensique »
- Développeur : Jakub Zawadzki
  - Tuteur : G. Arcas
- Travail sur fichier et non en mode Capture
- WireShnork : interface entre Wireshark et Snort
  - Introduit un nouveau Display Filter
  - Mots-clefs : snort, snort.sid, snort.msg
- WireAV : interface entre Wireshark et ClamAV
- WireViz : interface entre Wireshark et GraphViz
- http://honeynet.org/gsoc/slot8



- Cuckoo : sandbox pour analyse automatique de logiciels malveillants ou suspects en environnement Windows virtualisé
  - Développé en Python au-dessus de VirtualBox et d'un WM Windows.
- Principes :
  - Automatise le lancement de la VM, le transfert du binaire de la machine Hôte à la machine Invité et le lancement de ce binaire.
    - Supporte aussi l'analyse de fichier MS Office et PDF si logiciels installés.
  - Génère et stocke les traces issus de la VM :
    - Fichiers installés, clefs de registre, traces Réseaux.
    - Résultats accessibles via un serveur Web intégré à Cuckoo.
  - http://cuckoobox.org/
  - Cuckoo en ligne : http://malwr.com

About me...

- Consultant Sekoia
  - guillaume.arcas@sekoia.fr

- The Honeynet Project
  - Co-Chapter Lead French Chapter
  - Chief Public Relations Officer
    - project@honeynet.org

- OSSIR
  - guillaume.arcas@free.fr