Anti-Anti-Sandbox

Notwendigkeit einer nicht detektierbaren Sandbox Umgebung

Einleitung

- Analyse von Schadprogrammen
  - Sandbox Umgebung / automatische Analyse
  - Wir möchten bspw. die Rückkanalwege erkennen
- Problem
  - Spionageprogramme sind häufig „zugeschnitten“
  - Kein entsprechendes Verhalten wenn die Umgebung nicht „stimmt“

Anti-Sandbox Methoden

- Detektion der Virtualisierung
  - Nicht das eigentliche Problem
    - Virtualisierte Server können auch Ziel sein
    - Häufig Simulation eines Büro-Rechners
  - Sandbox-Umgebung muss mit Ziel übereinstimmen
  - Alle Komponenten müssen stimmen!
    - Beispiel Büro-Rechner:
      - Seriennummern von Speicherbaustein, Bildschirm, etc.
      - Konfiguration muss passen (CPU, Speicher, etc.)

Wie eine Sandbox aussehen muss / Ausblick

- Jede Virtualisierungsoftware hat ihre Eigenarten
- Beispiel VirtualBox
  - Hardening notwendig
    - MAC Adressen
    - BIOS Werte überschreiben
    - Seriennummern bereitstellen
    - „Hypervisor present bit“ (Paravirtualization Legacy verwenden)
  - Skripte für jede Umgebung verwenden
    - „vboxmanage setextradata …“
- …keine abschließende Untersuchung

Vielen Dank für Ihre Aufmerksamkeit