Восстановление адресного пространства процесса из расширенного образа памяти на платформе Windows

Овчинников Антон (445)

Научный руководитель:

ст. преп. Губанов Ю.А.

12 мая 2012

Задачи

Восстановление пользовательского адресного пространства процесса, используя:

- Образ памяти
- Расширенный образ памяти

Проблемы классического компьютерного криминалистического анализа
(digital forensics)

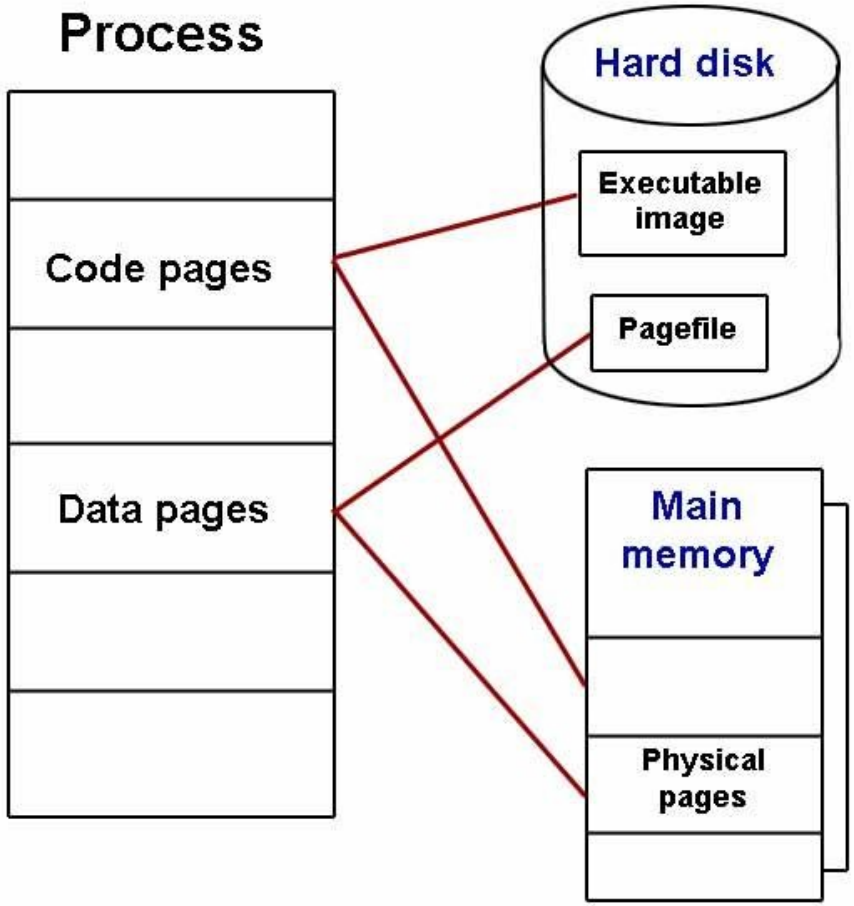
- Облачные технологии
- SSD-диски
  - Команда TRIM
- Шифрование
- Вредоносное ПО
  - Упаковка, антиотладка

Расширенный анализ памяти

Задача: полное восстановление адресного пространства процесса (ОС Windows)

Требуются:

- Образ памяти
- Файлы подкачки
- Файл образа
- Динамические библиотеки



Этапы и результаты

- Поиск структур

  EPROCESS, Page Directory (сигнатурный метод)

- Поиск страниц из разных источников
- Объединение адресного пространства

  Тестирование: восстановилось около 97% адресного пространства

- Восстановление данных

  Картинки, отображенные базы...

Этапы и результаты

- Из “сырого” образа

- Из восстановленного адресного просранства

Трудности и дальнейшее развитие

- Поиск устойчивых сигнатур
  - Зависимость от версии, ОС
- Адресное пространство ядра
- Исследование образа с виртуальной машиной