Восстановление памяти виртуальной машины из расширенного образа памяти базовой системы на платформе Windows

Овчинников Антон, 545 группа

Научный руководитель: ст. преп. Ю.А. Губанов

Рецензент: ст. преп. И.В. Зеленчук

13 июня 2013

Компьютерный криминалистический анализ (digital forensics)

- Анализ жесткого диска
- Анализ истории (браузеров, серверов)
- Анализ памяти
  - Облачные технологии
  - Шифрование
  - Вредоносное ПО

Анализ памяти и виртуализация

Использование виртуальных машин:

- Быстрое создание "чистой", переносимой среды
- Серверная виртуализация (Xen, KVM...)

Невозможно применить классические методы анализа памяти

Постановка задачи

Исследование запущенной виртуальной машины на основе образа памяти

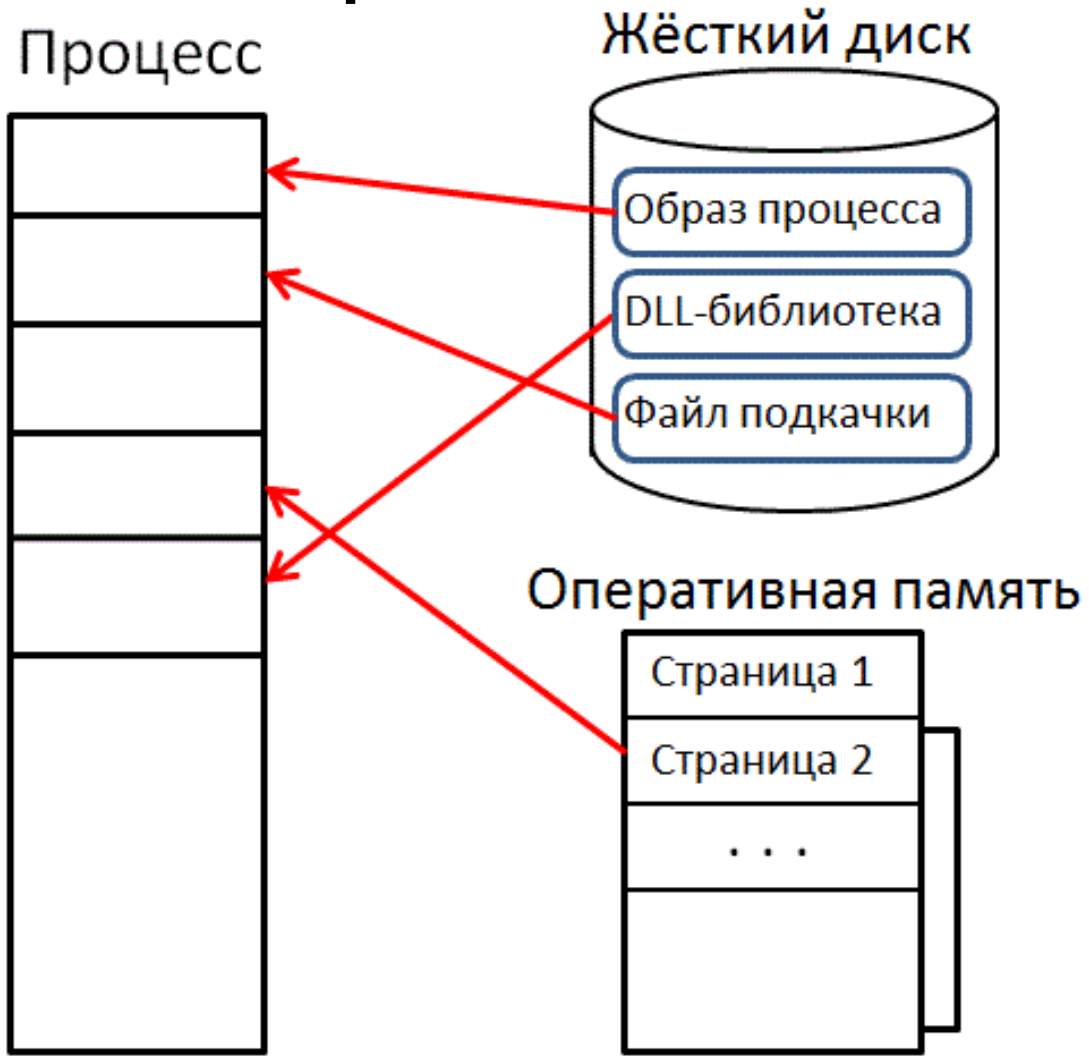
- Восстановление адресного пространства процесса виртуальной машины
- Восстановление физической памяти гостевой системы

После - можно использовать стандартные техники анализа памяти

Восстановление адресного пространства процесса

Расширенный образ памяти:

- Образ памяти
- Файлы подкачки
- Исполняемый образ
- DLL-библиотеки



Виртуальное адресное пространство процесса

Анализ адресного пространства

1. Поиск структур, описывающих отображение памяти
   - Сигнатуры, строки-идентификаторы

2. Проверка корректности найденных структур
   - Связность структур данных

3. Восстановление физической памяти гостевой системы

4. Проверка корректности восстановленной памяти

Интеграция

Belkasoft Evidence Center:

Прототип (Ruby) ⟶ Внедрение (C++)

Трехуровневая архитектура:

Результаты

- Разработана и реализована методика восстановления адресного пространства процесса из расширенного образа памяти ОС Windows 7
- Восстановлена физическая память гостевой системы средств виртуализации QEMU и VirtualBox
- Результаты внедрены в коммерческий продукт