ИНТЕРАКТИВНЫЙ АНТИРУТКИТ

Магистерская диссертация студента 661 группы
Королева Дмитрия

Научный руководитель: ст. преп. Ю.А.Губанов
Рецензент: лидер клуба ХакерДом И.В.Зеленчук

Существующие решения

- Брандмауэр
- Системы обнаружения вторжений (Intrusion-Detection System, IDS)
- Системы предотвращения вторжений (Intrusion-Prevention System, IPS)

При обнаружении подозрительных действий программ, нет возможности дальнейшего анализа аномалий

Постановка задачи

1. Провести обзор подходов к поиску руткитов на компьютерах пользователей
2. Провести сравнительный анализ существующих инструментов для анализа руткитов
3. Выявить набор признаков присутствия руткитов
4. Реализовать инструмент, позволяющий детектировать эти признаки и предоставляющий возможность проводить дальнейший анализ аномалий
5. Убедиться в его работоспособности на существующих видах руткитов

WinDBG

- Автоматический разбор структур Windows
- Использует свои библиотеки
- Автоматическая загрузка файлов отладочных символов
- Множество встроенных команд отладки

Методы обнаружения руткитов

- Использование альтернативного доверенного окружения
- Поведенческий метод
- Метод сигнатур
- Детектирование перехватов
- Сравнение данных из различных источников
- Аппаратный метод
- Проверка целостности
- **Анализ образов памяти**
- Гипервизор

Алгоритмы для реализация

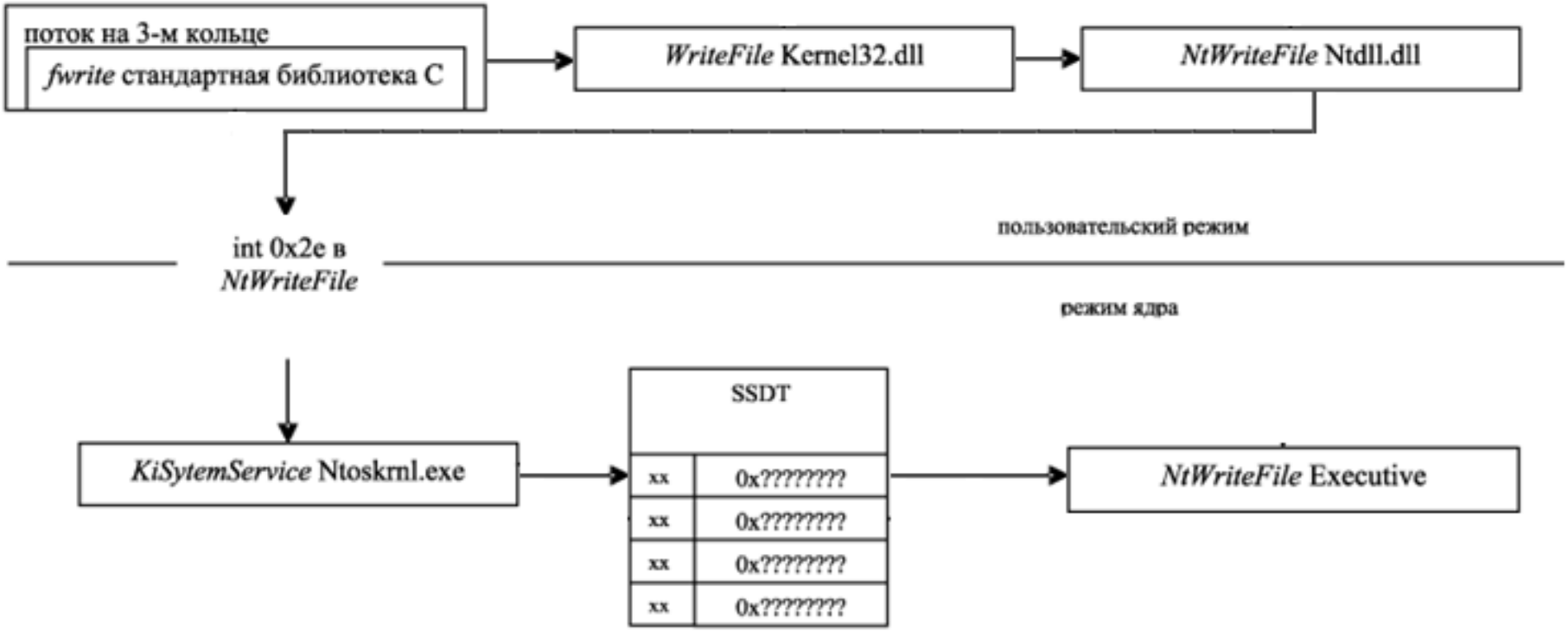
- Поиск скрытых загруженных в память модулей
- Обнаружение перехватов функций в SSDT
  - Изменение указателей функций в SSDT
  - Подмена указателя на SSDT в исполняемых потоках
- Обнаружение скрытых процессов

1. Поиск скрытых загруженных в память модулей

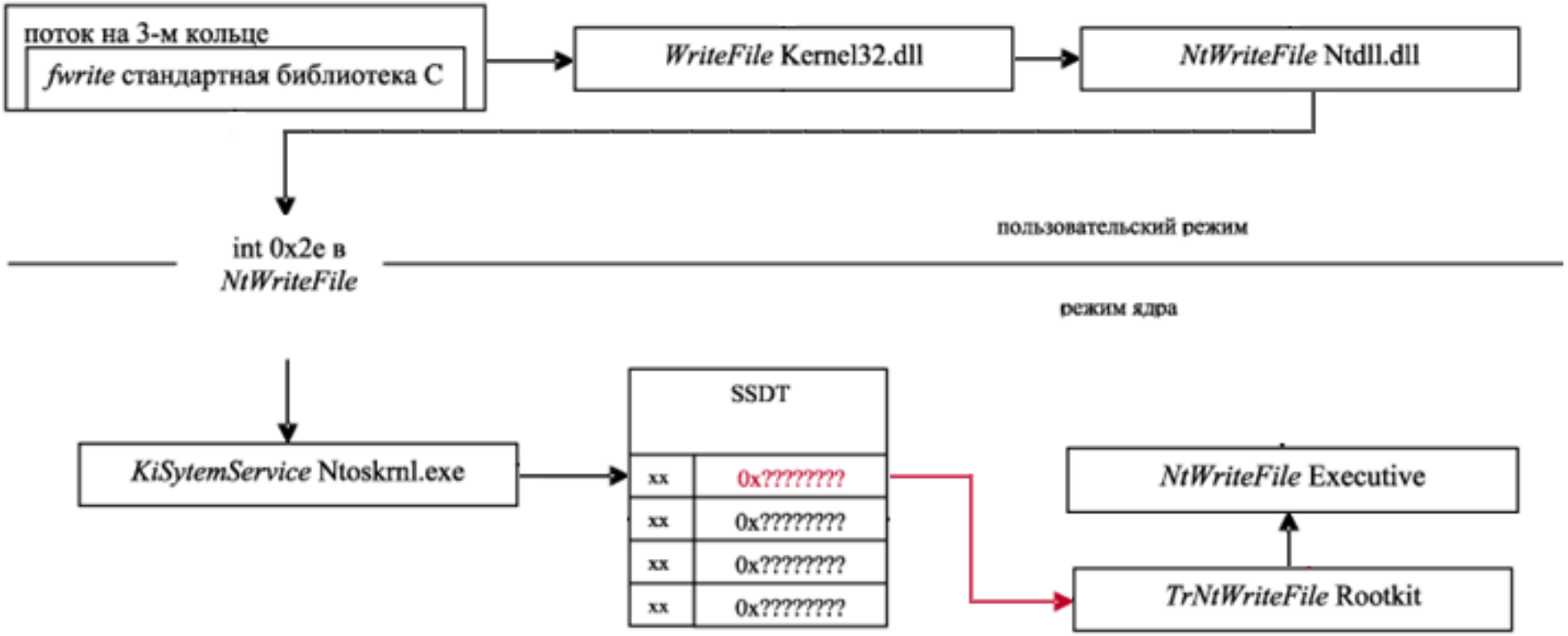
- Поиск исполняемых модулей по их заголовку формата MZ-PE
- Получение информации о найденном модуле, с помощью команды «!lmi»

- Процесс автоматизирован для всех найденных заголовках MZ

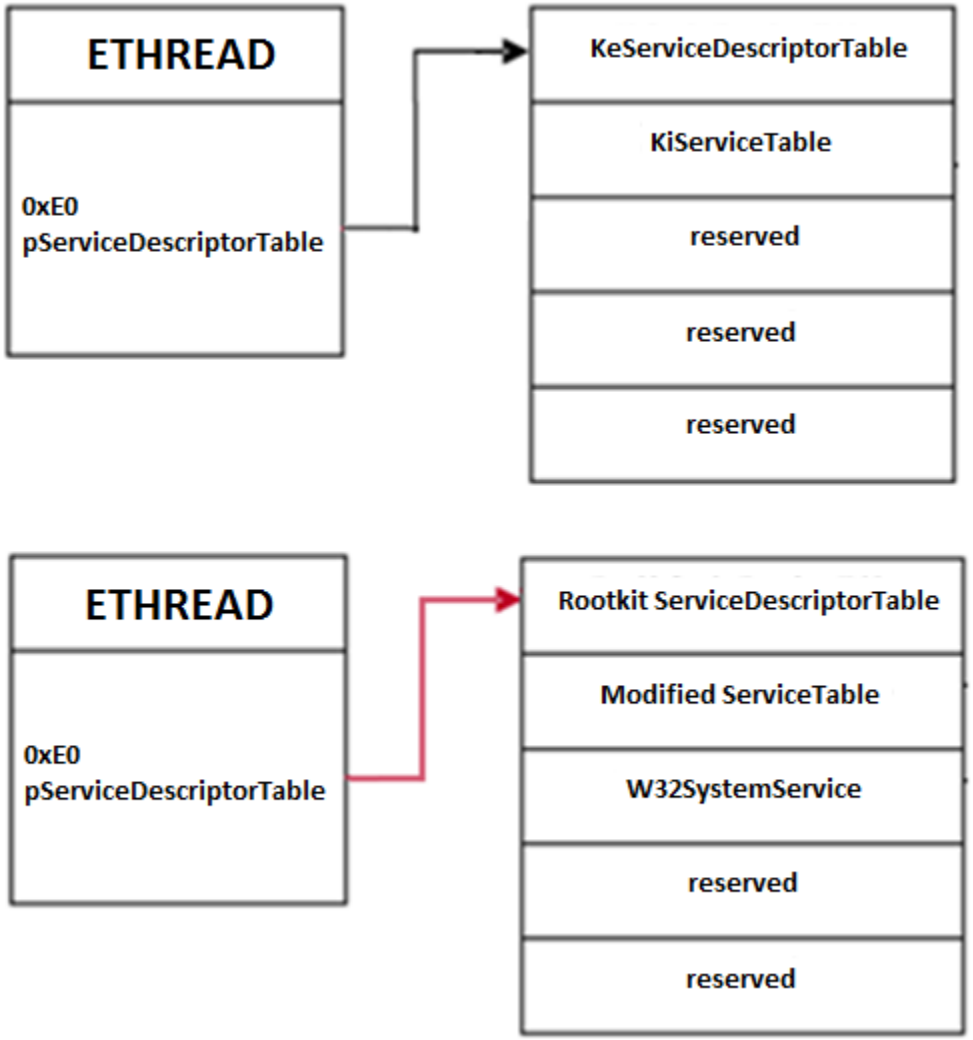
2. Обнаружение изменения указателей функций в SSDT



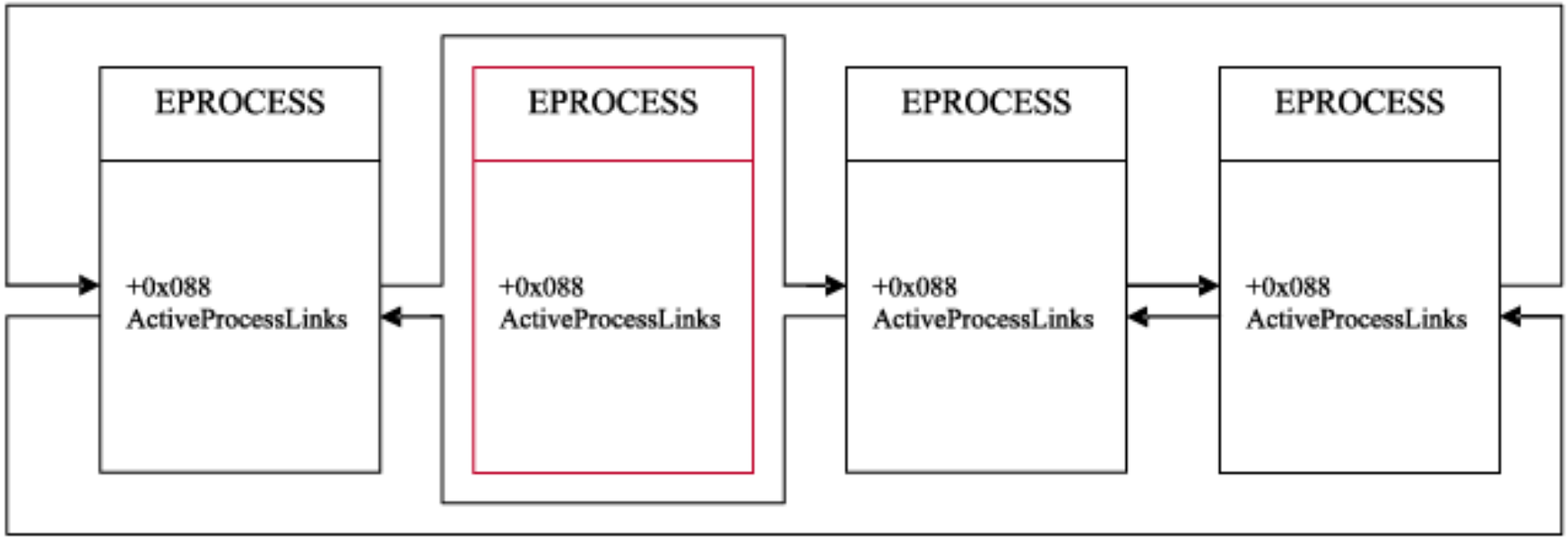
2. Обнаружение изменения указателей функций в SSDT



3. Обнаружение подмены указателя на SSDT в исполняемых потоках



4. Обнаружение скрытых процессов



Реализация. Скрипты

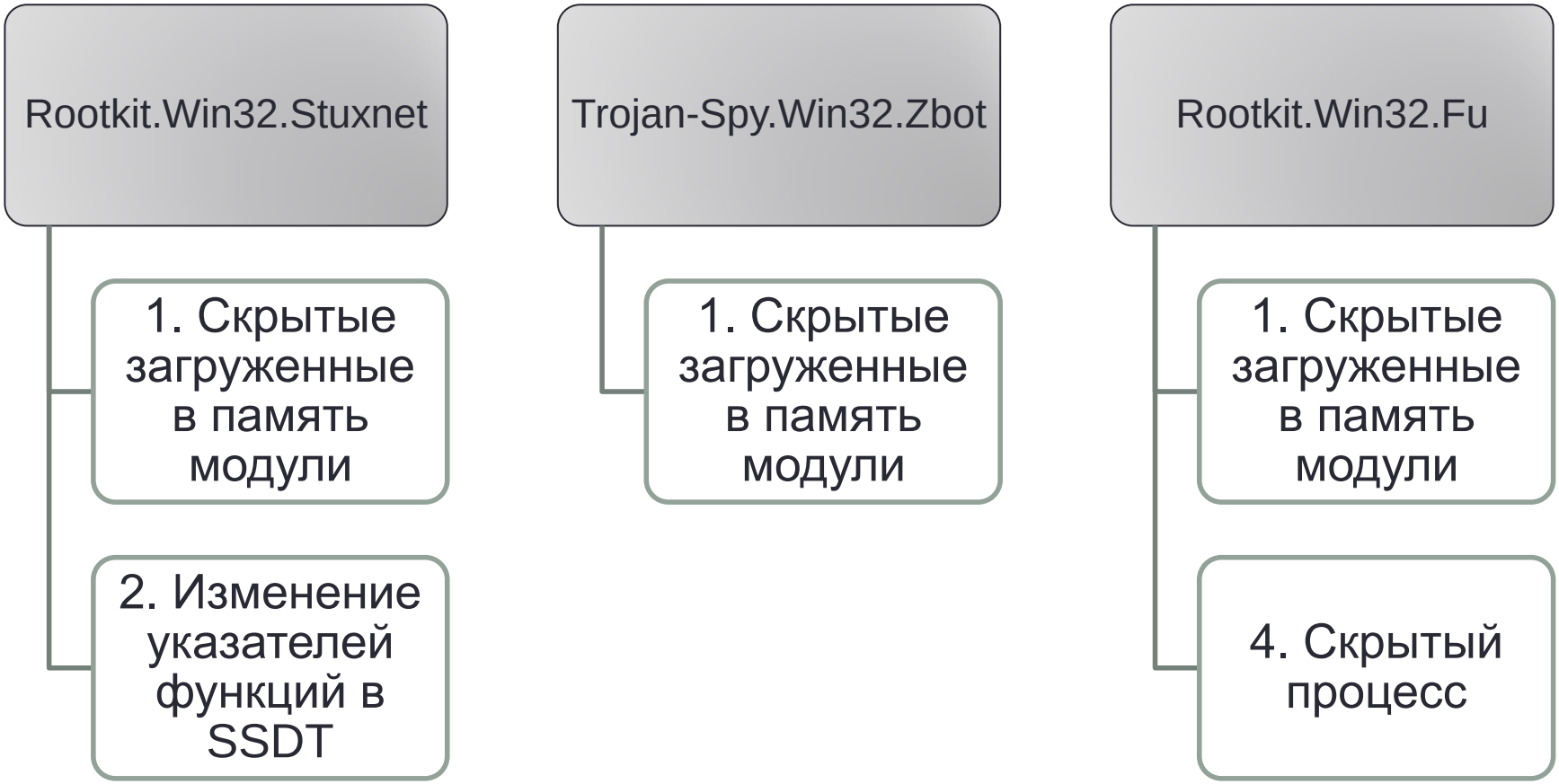
- search_hidden_modules
- search_hidden_process
- SSDT_calls
- SSDT_in_threads

```
$$ Iterate Threads
.for (r $t4 = poi(@$t3);
      (@$t4 != 0) & (@$t4 != @$t3);
      r $t4 = poi(@$t4))
{
    r? $t5 = #CONTAINING_RECORD(@$t4, nt!_ETHREAD, ThreadListEntry)

    r? $t5 = (nt!_KTHREAD *)@$t5

    $$ Calculating offset of KTHREAD::ServiceTable
    r $t6 = @@c++(@$t5->ServiceTable)
```

Реализация. Окружение

- VMware Workstation 7.1.4;
- XP Professional;
- WinDbg 6.1.

Реализация. Результаты



Результаты

1. Проведен обзор подходов к поиску руткитов на компьютерах пользователей
2. Проведен сравнительный анализ существующих инструментов для анализа руткитов
3. Выявлен набор признаков присутствия руткитов
4. Реализован инструмент, позволяющий детектировать эти признаки и предоставляющий возможность проводить дальнейший анализ аномалий
5. Работоспособность алгоритмов подтверждена на поиске существующих видов руткитов