Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Современный RE:
кому он нужен и чем занимается

Дмитрий Скляров,
Head of Reverse Engineering, Positive Technologies

Синтез vs Анализ

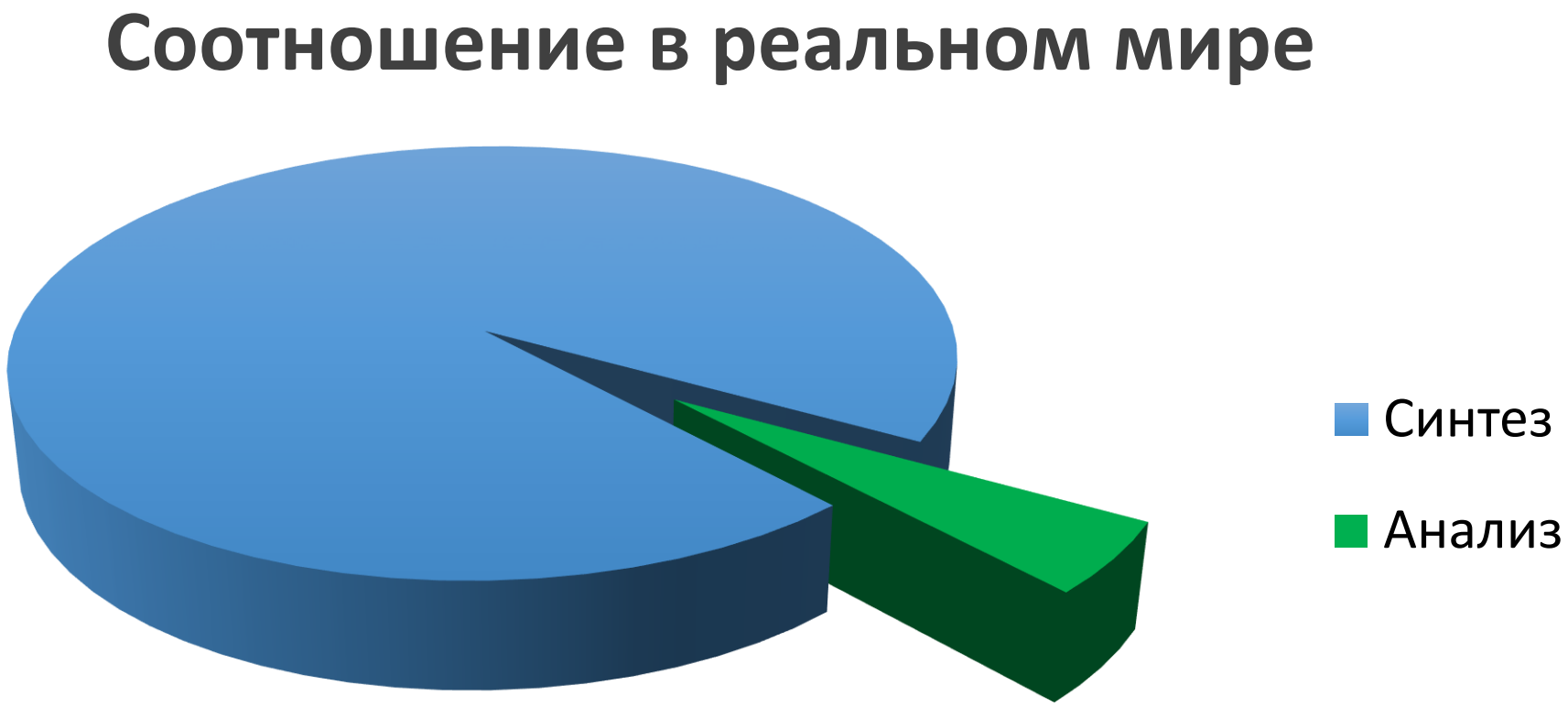
Задачи синтеза

- Из базовых блоков построить решение с требуемым функционалом
- Придумать новый базовый блок
- Разработать систему правил для обеспечения необходимых ограничений
- Проверить отсутствие нарушений правил

Задачи анализа

- Разобрать решение на базовые блоки
- Описать функционал неизвестных базовых блоков
- Обнаружить неполноту в системе правил
- Придумать способ обойти ограничения не нарушая при этом правила

Reverse Engineering – чистый анализ



Ты помнишь,
как все начиналось?

Зачем RE был нужен лично мне?

- Сделать бесконечное число жизней в игре
- Понять, почему Агат-отладчик грузится в несколько раз быстрее, чем Агат-DOS, хотя занимает ровно столько же
- Получить возможность заглянуть в «черный ящик»
- Заставить программу работать не так, как хотел автор

Такие разные применения RE

Светлые

- Обеспечение совместимости с недокументированным ПО
- Восстановление забытых паролей
- Борьба с вредоносным ПО
- Анализ ПО на наличие НДВ
- Аудит безопасности ПО

Темные

- Кража интеллектуальной собственности
- Несанкционированный доступ к информации
- Разработка методов обхода антивирусов
- Жульничество в играх

Но совершенно одинаковые методы и инструменты!

Куда податься реверсеру в конце XX века?

- Анализ вредоносного ПО
- Анализ ПО на наличие «закладок»
- Обеспечение совместимости с неподдерживаемым ПО
- Password Recovery

Особенности исследуемых объектов

Процессор

- Преимущественно x86

Операционная система

- Преимущественно Windows
- Иногда DOS

Возможности отладки

- Почти всегда доступна
- Иногда применяются анти-отладочные приемы

Популярные инструменты

- SoftICE
- OllyDBG
- Turbo Debugger
- Interactive Disassembler

Новые технологии шагают по планете

Технологии меняют ландшафт

Широкое распространение интернета

- К общедоступным сетям подключают все подряд

Развитие микроэлектроники

- Появляются тысячи новых энергоэффективных и компактных устройств

Беспроводные решения

- Удобно все хранить в Облаке и пользоваться откуда угодно

Время искать уязвимости…

- Операционные системы
- Браузеры
- Прикладное ПО
- Промышленные контроллеры
- Сетевое оборудование
- Мобильные устройства
- IoT
- …

Фаззинг

- Разновидность тестирования
- Требует много вычислительных ресурсов
- Позволяет автоматизировать поиск ошибок реализации
- Дает информацию для дальнейшего [ручного] анализа

Отладка «в прошлом»

- Сохраняется последовательность изменений состояния исследуемого объекта
- Можно «путешествовать во времени» и анализировать состояние в нужный момент

https://qira.me/

https://www.tetrane.com/

https://blogs.msdn.microsoft.com/windbg/2017/09/25/time-travel-debugging-in-windbg-preview/

Отладка из гипервизора

- Можно отлаживать ядро операционной системы не беспокоясь за его целостность

- Артефакты отладки [почти] невидимы для объекта исследования

https://github.com/honorarybot/PulseDbg (Артем Шишкин)

angr

- Дизассемблирование
- Инструментация (Program instrumentation)
- Символическое исполнение (Symbolic execution)
- Анализ потока управления (Control-flow analysis)
- Анализ зависимости данных (Data-dependency analysis)
- Анализ присвоения значений (Value-set analysis)
- Декомпиляция

https://github.com/angr/angr

Развитие дизассемблеров

- IDA Pro + HexRays
  https://www.hex-rays.com/

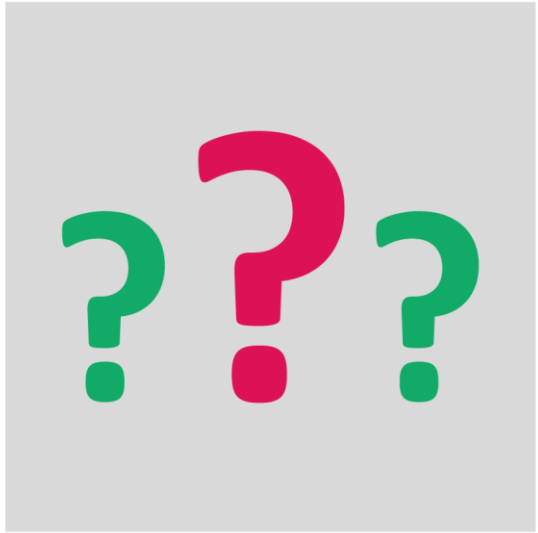
- Radare2
  https://rada.re/

- GHIDRA
  https://www.nsa.gov/resources/everyone/ghidra/

Реверсерам хватает работы…

- Анализ без возможности отладки
  - Иногда есть JTAG
  - Иногда возможна частичная эмуляция
- Анализ прошивок
  - Недокументированный формат
  - Произвольная архитектура CPU
  - Любая операционная система
- Получение прошивок
  - Все чаще требуется помощь человека с паяльником…
  - Полезно иметь электронный микроскоп ;)

Вопросы?



Современный RE:
кому он нужен и чем занимается

Контактная информация

Электронная почта:

DSklyarov@ptsecurity.com

Телефон:

+7(495)744-0144

Facebook:

www.facebook.com/PositiveTechnologies

Сайт:

www.ptsecurity.com