Невидимость исполняемого кода в Windows NT

Гилязов Руслан Раджабович
Смышляев Станислав Витальевич

Введение

КРИПТО ПРО

Невидимость исполняемого кода

Определение

Руткит – это набор программ, обеспечивающих постоянное, устойчивое и неопределяемое присутствие на компьютере.

Руткиты

Задачи, решаемые руткитом:

- внедрение
- запуск
- применения техник сокрытия.
  Объекты сокрытия могут быть:
  процессы, потоки, ключи реестра,
  файлы, папки и т.п.
- устойчивость присутствия

Типы руткитов

- **Уровень пользователя**
- **Уровень ядра**
- **Гипервизор**
- **SMM**
- **Микрокод**

Рутkиты уровня пользователя

Простая, старая технология. Обнаруживается легко. Разрабатывается легко. Плюсы в том, что ниже требования к СРД(обычно требуется меньше прав).

Руткиты уровня ядра

Сплайсинг SSDT, установка драйвер фильтров, сплайсинг драйверов, модификация объектов ядра(DKOM), IDT и т.п. элементов ОС. Наиболее распространенные и практически применимые технологии.

Рутkиты гипервизоры

ОС ставиться поверх гипервизора. Технологии виртуализации, которые поддерживают современные процессоры предоставляют потенциальные возможности по контролю функционирования операционной системы.

SMM-руткиты

Во время функционирования вычислительного устройства поддерживающего данную технологию происходит регулярное, интенсивное использование SMM технологии. SMM код получает доступ ко всей системной памяти, включая ядро и память гипервизора

Микрокод

Некоторые современные материнские платы имеют чипсет vPro-compatible MCH, у которого есть отдельный процессор, ОЗУ и ПЗУ. AMT код выполняется независимо от кода, выполняющегося на центральном процессоре компьютера, кроме того AMT может напрямую взаимодействовать с сетевой картой, что позволяет создавать неконтролируемые из программной среды работающей на центральном процессоре каналы связи. Кроме того AMT код может оказывать влияние и контролировать код, исполняющийся на центральном процессоре.

Закладки в микрокоде устройств

Детектирование

- Несоответствие ответов на эквивалентные информационные запросы
- Контроль целостности
- Сравнение с эталоном
- Сигнатура
- Эвристика
- По косвенным признакам

Построение модели

Цели:

1. Теоретическое и практическое описание невидимых модулей КС
2. Теоретическое и практическое описание технологий детектирования модулей невидимости КС
3. Оценка защищенности операционной системы типа Windows NT от невидимых модулей
4. Общая оценка эффективности существующего защитного программного обеспечения для операционной системы типа Windows NT от невидимых модулей

Модель

Введено понятия модуля. Выделены три состояния, в которых может находится модуль: active, loading, on_hold

2. Введено понятие невидимости исполняемого кода
3. Введено понятие технологии сокрытия
4. Введены уровни функционирования исполняемого кода

Модель

Модуль A^{active} является невидимым для модуля B^{active}, если:

1. A - применяет технологию сокрытия
2. A - находится на уровне ниже B,

либо на таком же уровне в случае, если A - загрузился раньше B

Модель

КРИПТО ПРО

Модуль B^{active} может обнаружить модуль A^{active}, если:

1. A - применяет технологию сокрытия
2. B - находится на уровне ниже A, либо на таком же уровне в случае, если B - загрузился раньше A
3. A - существует на момент функционирования B

Модель

Модуль A^{on_hold} является невидимым для модуля B^{active}, если:

не существует алгоритма R, используя который модуль B мог бы по методу сигнатурного поиска найти признаки реализации технологии сокрытия в модуле A

Модель

Модуль A^{loading} является невидимым для модуля B^{active}, если:

не существует алгоритма R, используя который модуль B мог бы по методу эвристического анализа найти признаки реализации технологии сокрытия в модуле A

Результаты из модели

Требования к ЗПО(ВПО):
1)Работать на максимально технологически возможном низком уровне.
2)Контролировать вход на уровень ЗПО(ВПО)
3)Обеспечивать целостность ЗПО(ВПО) до момента его активации.

Результаты из модели

В качестве ЗПО достаточно СРД, которая действует на все уровни ниже, уровня на котором работает ЗПО и системы контроля загрузки на уровень, на котором работает данное ЗПО

Результаты из модели

Даже если модель будет соблюдена,
на практике актуальным остается
проблема небезопасности
используемых языков
программирования.

Результаты модели

Построенный компонент

КРИПТО ПРО

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru
rubin@cryptopro.ru
svs@cryptopro.ru

Тел./факс:
+7 (495) 780-48-20
+7 (495) 660-23-30