Применение антивирусных программных средств в расследовании инцидентов информационной безопасности.

Юрий Резников,
руководитель группы
по работе с клиентами
ОДО "ВирусБлокАда"

Расследование инцидентов: порядок действий

- Что подозрительно?
- Можно ли справиться самостоятельно?
- Как предотвратить подобные ситуации в будущем?

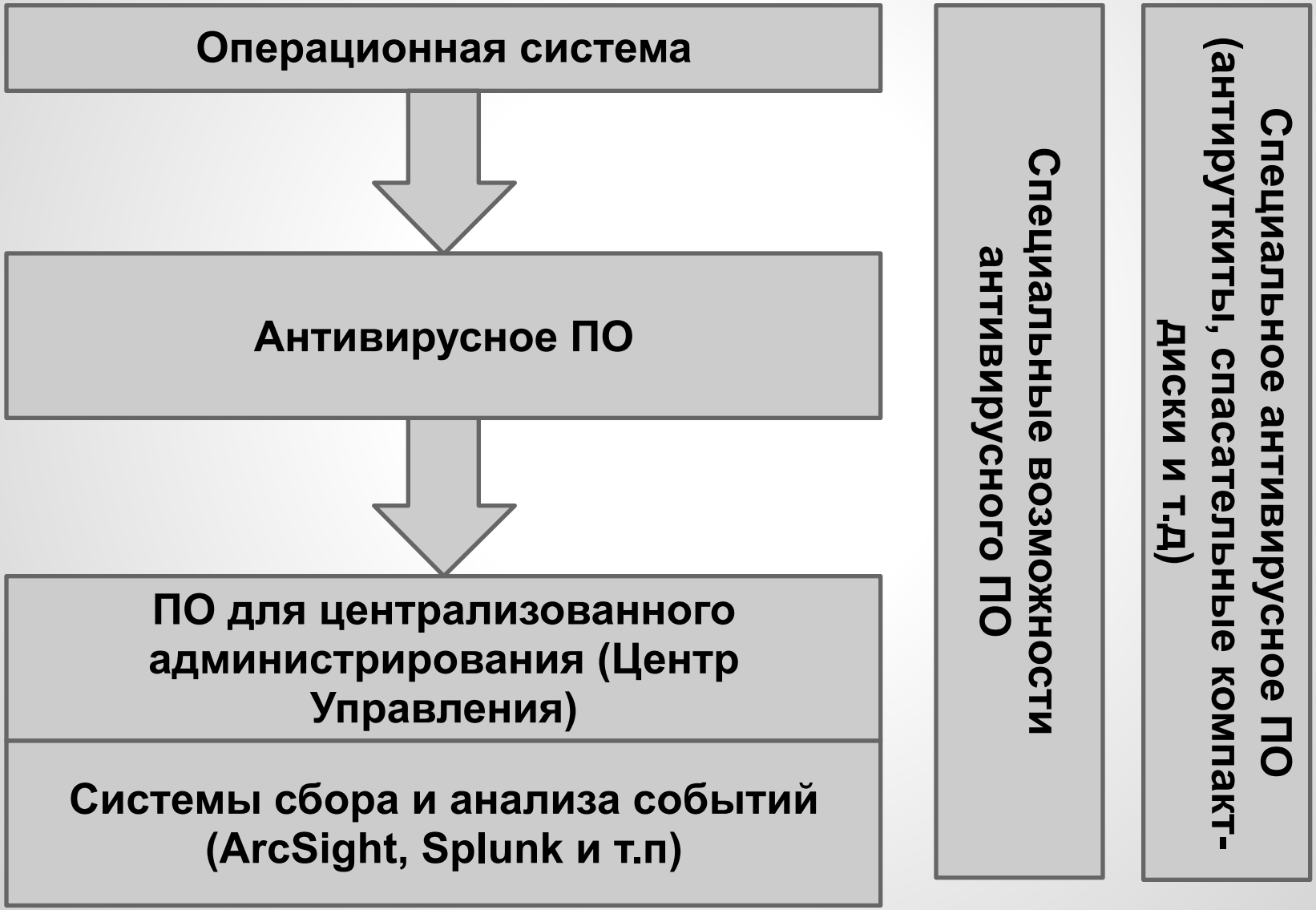
Обнаружение подозрительных ситуаций

- Защита периметра
- Централизованный сбор событий безопасности
- Обработка событий безопасности антивирусного ПО
- Уведомление сторонней организации

Задачи средств антивирусной защиты при расследовании инцидентов

- Предоставить информацию об инциденте, достаточную для начала расследования
- Позволить провести анализ ситуации в ходе расследования
- Принять меры для предотвращения подобных ситуаций в будущем (позволить проанализировать информацию + отправить информацию компании-разработчику средств защиты).

Как собирать информацию об инциденте?



Расследование инцидентов безопасности с помощью журналов ОС

- Вероятное использование уязвимостей (пример: Worm.Win32.Kido). НЕОБХОДИМ ОПЫТ!!!
- Аудит попыток входа в систему.
- Обнаружение конфликтов ПО.

Анализ журналов антивируса.

- Действенен, если компьютер не подключен к сети
- Есть вероятность обнаружить атаки на самозащиту антивируса
- Хорошо поддается автоматизации (легко обрабатываемые текстовые файлы)

Модуль Vba32 USB.

Поставляется в двух видах:

- С централизованным управлением
- С управлением на локальном (отдельно-стоящем компьютере)

Возможности модуля Vba32 USB

- Ограничение работы пользователя только авторизированными USB-флеш накопителями.
- Ведение отчета о выполненных операциях с файлами на USB накопителе.
- Интеграция с Vba32 Центром Управления.

Файл отчета модуля Vba32 USB

1. Название рабочей станции
2. Имя учетной записи
3. Время и дата события
4. Уникальные номер носителя или имя файла, действия над которым проводились
5. Действие проведенное с носителем информации или файлом (путь к файлу также указывается в отчете)

Пример отчета модуля Vba32 USB

SPY-PC VBADOMAIN\sbrych 18:15:03 18-10-2012 Inserted LG USB Drive AA04012700008617 вставлено
SPY-PC VBADOMAIN\sbrych 18:15:04 18-10-2012 Mounted LG USB Drive AA04012700008617 смонтировано
SPY-PC VBADOMAIN\sbrych 18:15:04 18-10-2012 UnMounted LG USB Drive AA04012700008617 извлечено
SPY-PC VBADOMAIN\sbrych 14:00:36 19-10-2012 Inserted HTC Android Phone HT9BXL902460
SPY-PC VBADOMAIN\sbrych 14:00:36 19-10-2012 Mounted HTC Android Phone HT9BXL902460
SPY-PC VBADOMAIN\sbrych 15:09:32 19-10-2012 Inserted silicon-power 11030638E6B31100BC410001
SPY-PC VBADOMAIN\sbrych 15:09:32 19-10-2012 Mounted silicon-power 11030638E6B31100BC410001
SPY-PC VBADOMAIN\sbrych 15:09:32 19-10-2012 UnMounted silicon-power 11030638E6B31100BC410001
SPY-PC VBADOMAIN\sbrych 14:51:41 30-11-2012 Inserted Apple Inc. iPod 000A270023083C0A
SPY-PC VBADOMAIN\sbrych 14:51:41 30-11-2012 Unknown Blocked Apple Inc. iPod 000A270023083C0A

Vba32 Центр Управления

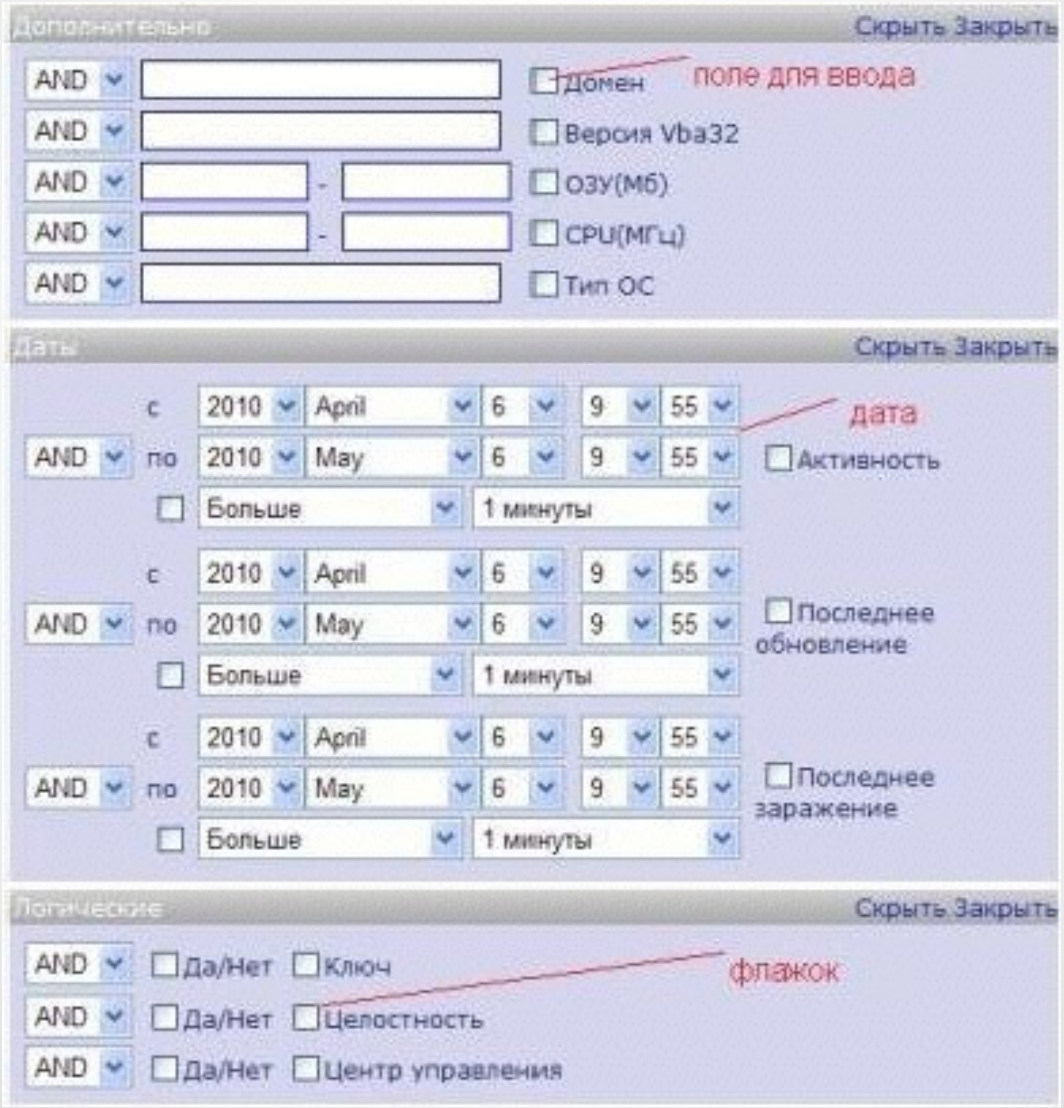
позволяет

- проводить постоянный мониторинг состояния компонентов антивирусного комплекса Vba32 на рабочих станциях;
- получить отчет о состоянии компонентов комплекса Vba32 на рабочей станции в сети;

Vba32 Центр Управления. Средства для расследования.

- Возможность удаленного запуска приложений на компьютере пользователя с правами системы
- Гибкая система фильтров

Vba32 Центр Управления. Система фильтров.



Case Study: вирусный инцидент. Расследование с помощью ЦУ.

Исходные данные: активное заражение на одном компьютере в сети. Остальные компьютеры заражению не подверглись, Центр Управления содержит множество событий virus.found и virus.cured

Ход расследования: анализ событий ЦУ показал, что очагом заражения является компьютер, который отправил событие loader.unloaded перед началом заражения.

Приняты административные меры.

Vba32 Antirootkit

Предназначен для глубокого анализа операционной системы и обнаружения и нейтрализации руткитов – программ, обеспечивающих постоянное, устойчивое и неопределяемое присутствие на компьютере. При этом осуществляется поиск как уже известных (добавленных в базу), так и неизвестных типов руткитов.

Возможности Vba32 Antirootkit

- Поиск аномалий в ядре ОС (модули ядра, перехваты системных вызовов, нотификаторы и т. д)
- Анализ запущенных процессов (загруженные и выгруженные модули)
- Поиск аномалий в реестре
- Доступ к файловой системе на уровне контроллера жесткого диска. И этом может проводиться проверка с помощью антивирусного ядра.

Возможности Vba32 Antirootkit

- Продвинутая система самозащиты (технология Vba32 Defender)
- Поддержка запуска программы на выделенном рабочем столе

Vba32 Antirootkit позволяет специалисту увидеть результат полного анализа системы и принять решение, необходимое для продвижения расследования инцидента

Vba 32 Remote Console Scaner

- Дополнительный продукт с централизованным управлением, не мешающий работе антивирусу основного вендора.
- Пользователь данного продукта получает дополнительную помощь в виде вирусных аналитиков и технической поддержки, что является плюсом при расследовании инцидентов.

НАШ ДЕВИЗ – ПОМОГАТЬ ВСЕМ И ВОВРЕМЯ!

СПАСИБО ЗА ВНИМАНИЕ