Независимый информационно-аналитический центр

Антивирусная защита сегодня
Большой технологический переход
или затыкание дыр?

Илья Шабанов
Управляющий партнер

Как это было раньше

- Сигнатуры для обнаружения вредоносных программ
- Гонка за обновлениями (количество в сутки, скорость реакции)
- Развитие проактивных технологий обнаружения (эвристика, поведенческий анализ)

Работа по черным спискам вредоносных программ.
Разрешено все, что не запрещено.

Проблемы черных списков

- Зависимость от постоянного пополнения базы данных
- Анализ на вредоносность – «узкое место» для антивирусных вендоров
- Лавинообразный рост количества новых вредоносных программ приводит к увеличению пропусков
- Увеличение сложности вредоносных программ

При текущих 200 тыс. новых вредоносов в сутки на черных списках не возможно построить надежную защиту

Что мы имеем сейчас

- Репутационные БД (файлы, URL, email)
- «Облачные» коллективные знания => пополнение репутационных БД
- Попытки перехода на белые списки
- Ограничение недоверенных программ
- Изолированные среды (песочницы)
- Интеграция с различными околоантивирусными технологиями
- Принуждение и ограничение прав (policy enforcement)

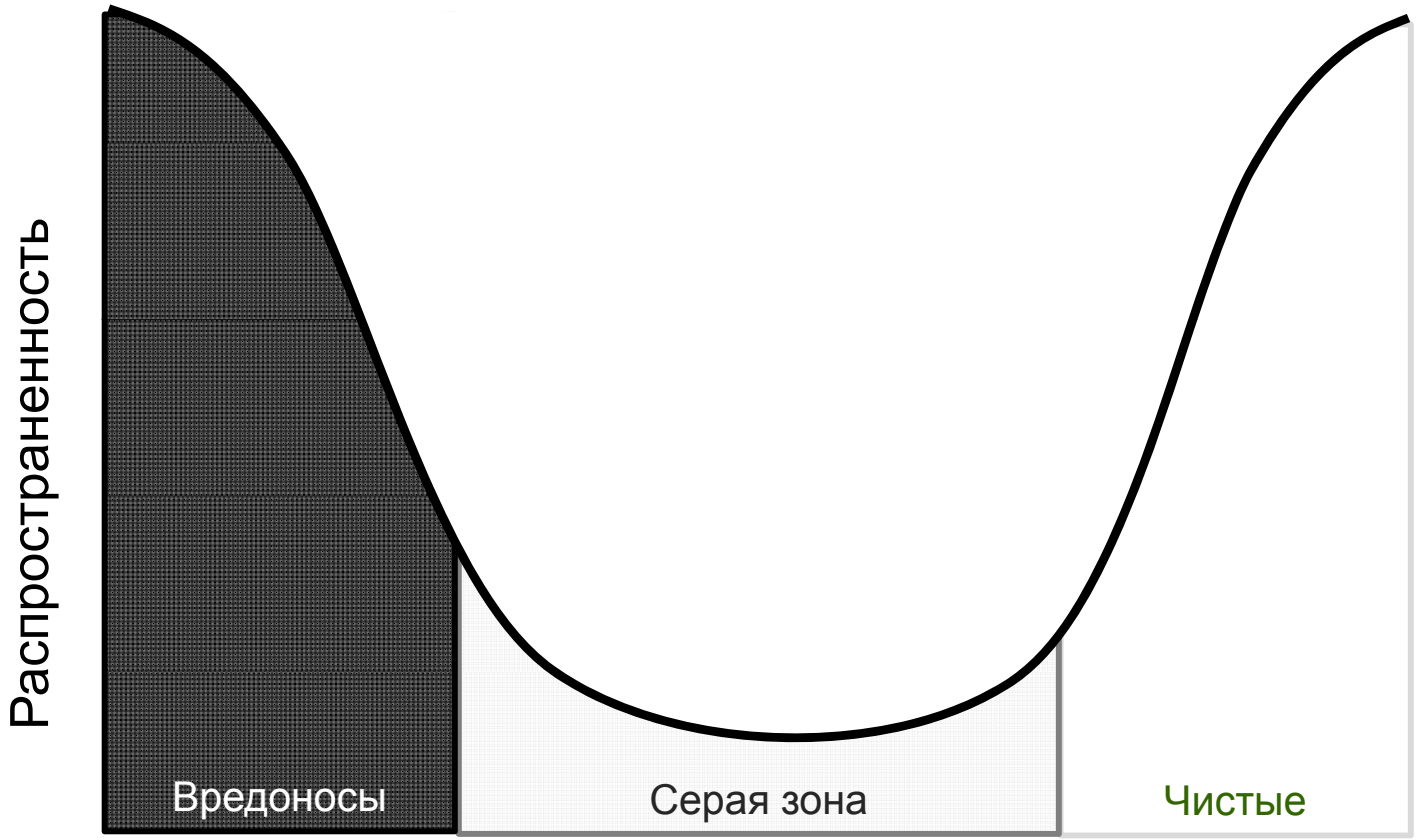
Проблемы белых списков

- Белые списки также нужно пополнять => все те же обновления
- Нужна категоризация программ
- Возникает проблема с обновлениями
- Малораспространенные программы рискуют попасть в опалу
- Возможен обман белых списков (компрометация «облака», цифровых подписей и т.п.)

Технология больше подходит для типизированных корпоративных рабочих мест с жестким набором ПО

Что делать с серой зоной?

Распределение программ по вредоносности



Защита, построенная на белых списках, принципиально не решает проблему, а лишь переводит ее на другой уровень

Существующие проблемы

- Недовольство пользователей (неудобно, лишние ограничения, «не как раньше»)
- Отторжение новых подходов
- Социальная инженерия
- Целевые атаки (APT)
- Мультиплатформенность
- Виртуализация и облака

Чего ждать в будущем?

Развитие технологий

- Работа с доверенной зоной и ПО из белого списка
- Полная изоляция или запрет недоверенного ПО
- Контроль целостности системы
- Compliance - соответствие правилам и политикам безопасности (обновление, настройки, права)
- Смещение акцента в сторону управления правами и политиками, классический антивирус перестает быть в центре защиты
- Строгая аутентификация и шифрование данных

ANTI-MALWARE

Спасибо за внимание!

Вопросы?

Илья Шабанов

Ilya.shabanov@anti-malware.ru

http://www.anti-malware.ru

Twitter: IlyaShabanov