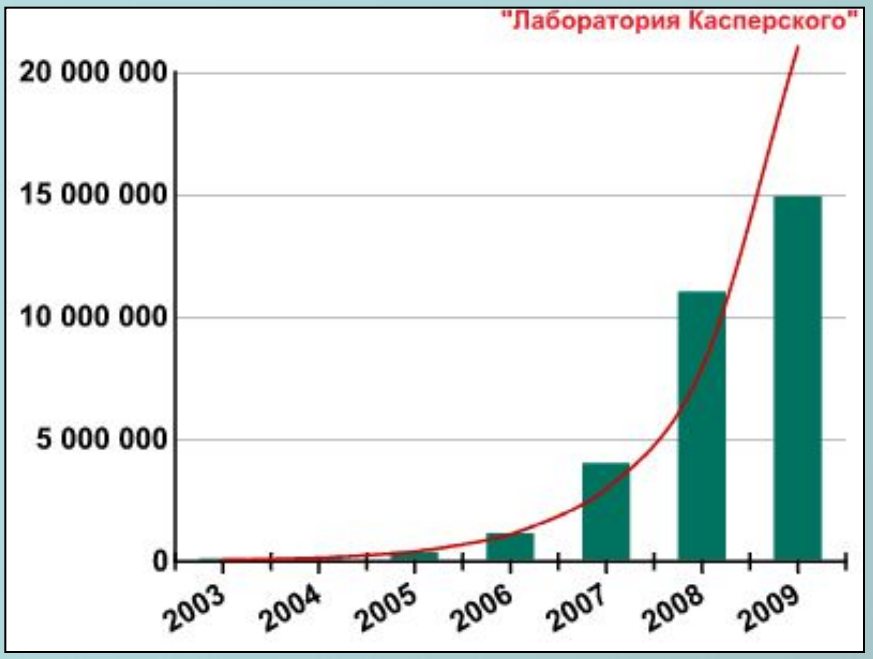
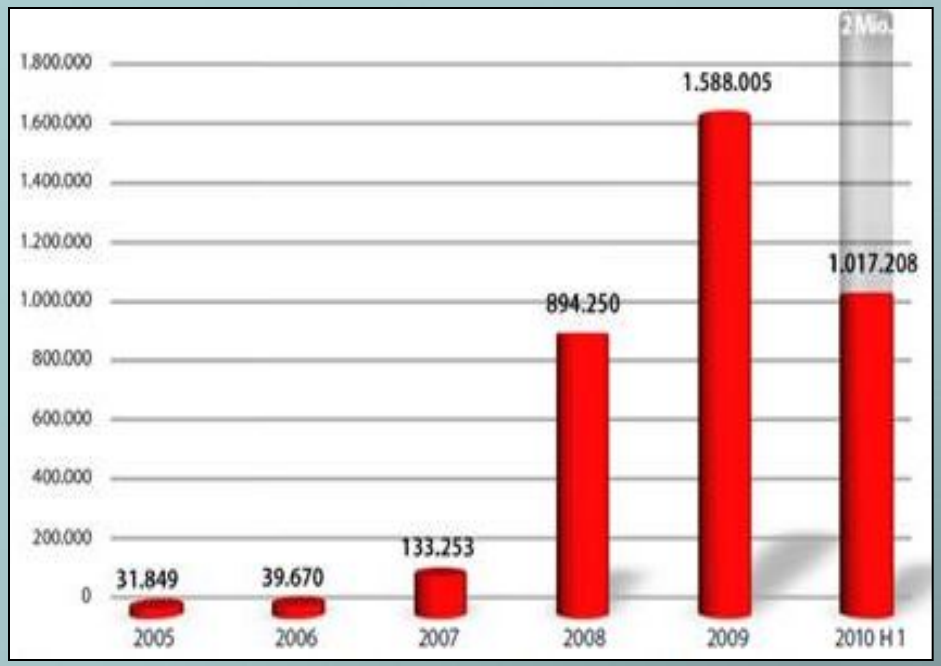
Почему бизнес на вредоносном ПО всё ещё существует?

Илья Рабинович, CEO
SoftSphere Technologies

Экспоненциальный рост продолжается.





Господствующая модель защиты.

- Решения на чёрных списках- «блокируем всё то, что подозрительно похоже на зловредные модули». Блокируют программные агенты.
- Реализация- антивирусы, продукты класса Internet Security и Total Security.
- Степень распространения- очень высокая (данные Eurostat- 84% в среднем по Европе за 2010 год).

Теневая модель заработка.

- Кража банковских данных и систем онлайновых платежей (логины, пароли, явки…).
- Продажа ресурсов заражённых компьютеров для организации DDoS, рассылок спама и анонимных прокси.
- Вымогательство.
- **Требует запуска программных агентов!**

Теневые доходы.

- Согласно последнему отчёту корпорации Symantec, совокупный доход теневого бизнеса достигает $114 миллиардов долларов.
- Бизнес на зловредном ПО- это преступление, но люди идут на него ради высоких прибылей. Намного более высоких, чем в легальном секторе экономики, есть риск сесть в тюрьму.

Доказательство.

- Бизнес на вредоносном ПО не может существовать при высоком уровне распространения защитных средств, если нет гарантированного и недорогого средства их обхода.
- То есть, **само существование бизнеса на зловредном ПО доказывает серьёзность проблем современных антивирусных средств в сфере предотвращения угроз**.

Насколько же хороша защита?

- В день создаётся, по разным оценкам, от 30 000 до 70 000 оригинальных вредоносных файлов в день.
- AV-Comparatives Whole Product Test- 99,3% блокирования угроз лидером.
- Отсюда имеем **от 210 до 490 пропущенных вредоносных файлов в день! И эта цифра растёт из года в год.** Большая часть инвестиций ушли в лечение заражения, а не в предотвращение угроз.

Что почём?

- А за что же платят пользователи средств безопасности? Они платят за чувство защищённости, а не за реальный уровень защиты! Тесты им нужны только для того, чтобы подтвердить верность выбора AV.
- Пример: антивирус AVG на Win Phone 7. Абсолютно бесполезен как антивирус, рассчитан на эксплуатацию страхов заразиться.

Виртуальное противостояние.

- Процветают и антивирусные компании, и компании киберпреступников. Активы растут и у тех, и у других.
- Когда полиция Италии начала борьбу с мафией, в течение десяти лет для преступников всё было кончено. Антивирусной индустрии более 25 лет. Почему же дело не сдвинулось с мёртвой точки?

Парадокс.

- Те компании, которые имеют ресурсы на полноценную борьбу с массовой киберпреступностью (в основном, крупные открытые акционерные компании), делают это недостаточно хорошо (акцент не на R&D, а на стоимости акций и выплате дивидендов), а у тех, кто хочет делать это хорошо (в основном, частные компании), недостаточно ресурсов.

Кто виноват и что делать?

- Кто виноват в подобной ситуации? Виноваты вы сами, пользователи средств безопасности.
- Те пользователи, которые устанавливают дополнительную альтернативную защиту, не основанную на чёрных списках, имеют значительно меньшую вероятность заражения компьютера.

Вопросы?

- И таки самое время иметь свой вопрос!