Скупой платит дважды…

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

Бесплатный сыр лежит в мышеловке.

Сегодня никого не удивить компьютерными зловредами. Данная проблема уже захлестнула пользователей домашних ПК. Производители программного обеспечения упорно уговаривают пользователей вовремя ставить все новые и новые «заплатки», а производство антивирусного программного обеспечения (ПО) превратилось в серьезный бизнес.

В своей новой операционной системе Windows 8 компания Microsoft заявила о наличии встроенного антивируса. Нужен ли он? Безусловно. Достаточен ли? Вот тут меня берут обоснованные сомнения.

В данной статье мы с вами попробуем проанализировать эффективность данного антивируса. На мой взгляд, сегодня мы с вами имеем следующие пути проникновения вредоносного ПО на домашних ПК:

- Интернет
- Электронная почта
- Сменные носители.

Проанализируем два из трех:

- Интернет:
    - Фишинг
    - Вредоносные ссылки
- Сменные носители

Для анализа были выбраны с помощью Kaspersky Internet Security следующие коллекции:

- Коллекция вредоносных ссылок (70 штук)
- Коллекция фишинговых ссылок (100 штук)

С сайта http://malware.pl была скачана коллекция вредоносного ПО (август 2012 года) в количестве 6318 файлов 1 560 855 207 байт.

Тестирование проводилось на ПК под управлением Windows 8 (версия 9200, релиз, взятая с http://technet.com)

Вначале немного статистики.

По данным «Лаборатории Касперского» (http://www.securelist.com/ru/analysis/208050763/Razvitie_informatsionnykh_ugroz_vo_vtorom_kvartale_2012_goda) во втором квартале 2012 года было отражено **434 143 004** атак, проводившихся с

интернет-ресурсов, размещенных в разных странах мира. Всего в данных инцидентах было зафиксировано **145 007** уникальных модификаций вредоносных и потенциально нежелательных программ. (Данная информация предоставлена пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.)

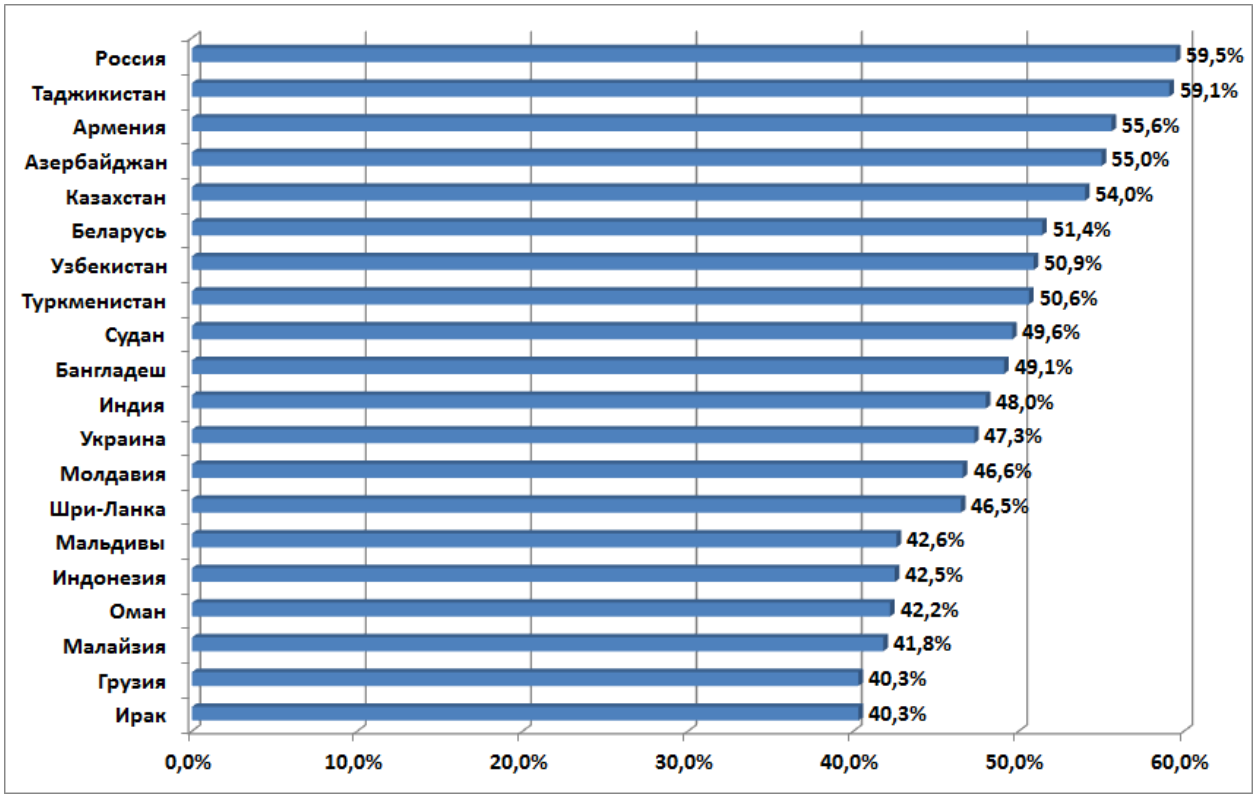

Рисунок 1 20 стран, где пользователи подвергаются наибольшему риску заражения через интернет*. Второй квартал 2012 г.

В TOP 20 преобладают страны - республики бывшего СССР, а также страны Африки и Юго-Восточной Азии.

Все страны можно разбить на несколько групп.

1. **Группа повышенного риска.** В эту группу с результатом 41-60% вошли 18 стран из TOP 20, в том числе Россия (59,5%), Казахстан (54%), Украина (47,3%), Индия (48%), Индонезия (42,2%) и Малайзия (41,8%).
2. **Группа риска.** В эту группу с показателями 21-40% попали 103 страны, в том числе Испания (37,8%), Италия (34,8%), Канада (36%), США (35,7%) и Англия (31,6%).
3. **Группа самых безопасных при серфинге в интернете стран.** В эту группу вошли 16 стран с показателями 12,3-20%.

Меньше всего процент пользователей, атакованных при просмотре страниц в интернете, на Тайване (15,2%), в Японии (18,1%), Дании (18,9%), Люксембурге (19,7%) и Чехии (20%).

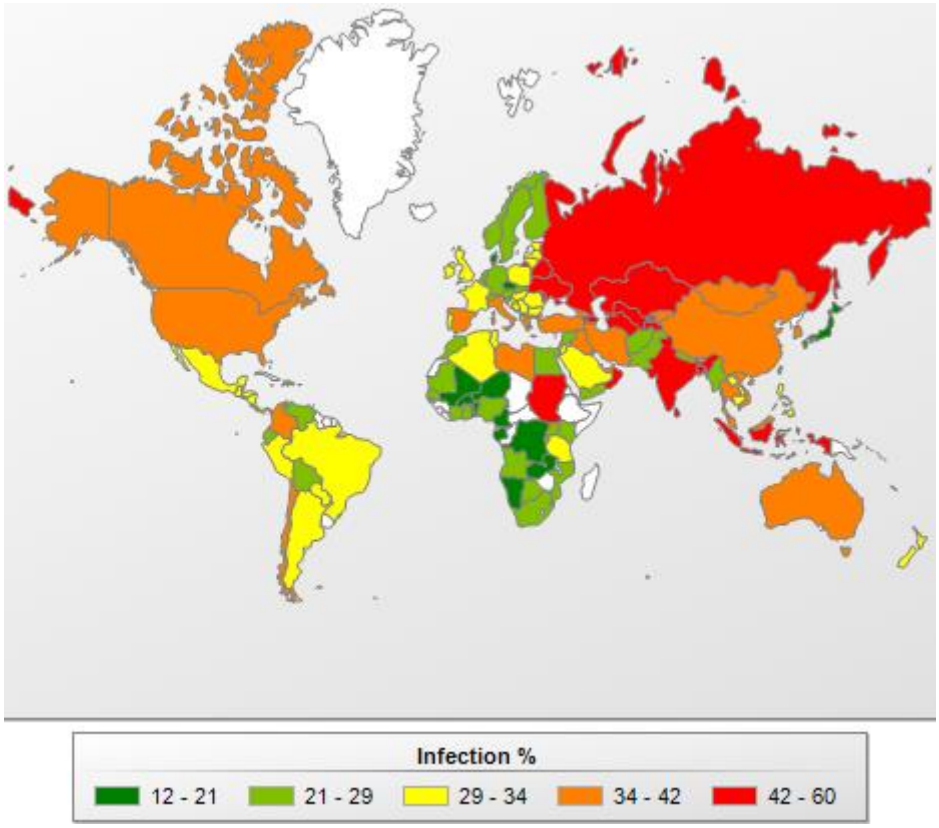

Рисунок 2 Риск заражения через интернет компьютеров пользователей в странах мира.

Давайте посмотрим, как же может нас защитить бесплатный встроенный в Windows 8 антивирус?

А вот тут, однако, мы имеем грустные цифры.

Вредоносные ссылки

Из представленных 60 вредоносных ссылок задержано с помощью Windows Defender всего 4.44%

Для сравнения был взят бесплатный антивирус AVG, версия которого с поддержкой Windows 8 была недавно представлена.

Из представленных 60 вредоносных ссылок задержано 8,89%, платная версия AVG Internet Security 2013 – 11,11% соответственно.

Еще раз напомню, коллекция собрана при помощи KIS 2013 (результат, соответственно 100%).

Грустно? Да нет, пожалуй, не грустно. Провально. Так будет вернее.

Фишинговые ссылки

В данном случае следует учесть, что фишинговые ссылки встроенный в Windows 8 антивирус отслеживать не умеет. Отслеживание фишинговых ссылок ведется с помощью Smart Filter, технологии, внедренной в Internet Explorer еще с версии 8.0. (т.е. пользователям альтернативных браузеров стоит об этом задуматься, ведь показатели фильтрования в браузерах, отличных от Internet Explorer будут заведомо куда хуже).

Итак, **Windows 8 со встроенным антивирусом задержано 88,37% фишинговых ссылок**

AVG Free – 90,7%

AVG Internet Security 2013 – 90,7%

Тестирование коллекции вирусов

В данном случае проверялся просто антивирусный сканер. Результаты откровенно удивили

	Windows Defender (Windows 8)	**AVG Free**	**AVG Internet Security 2013**	**Kaspersky Internet Security 2013**
Найдено	**17%**	**91,32%**	**91,32%**	**99,9%**

Таким образом, можно сделать вывод о том, что использование встроенного антивируса имеет смысл лишь как временная мера до установки платного специализированного ПО.