
TechDays.ru

Прогноз? Облачно!

Безмалый В.Ф.
MVP Consumer Security
Microsoft Security Trusted Advisor
http://bezmaly.wordpress.com
vladb@windowslive.com

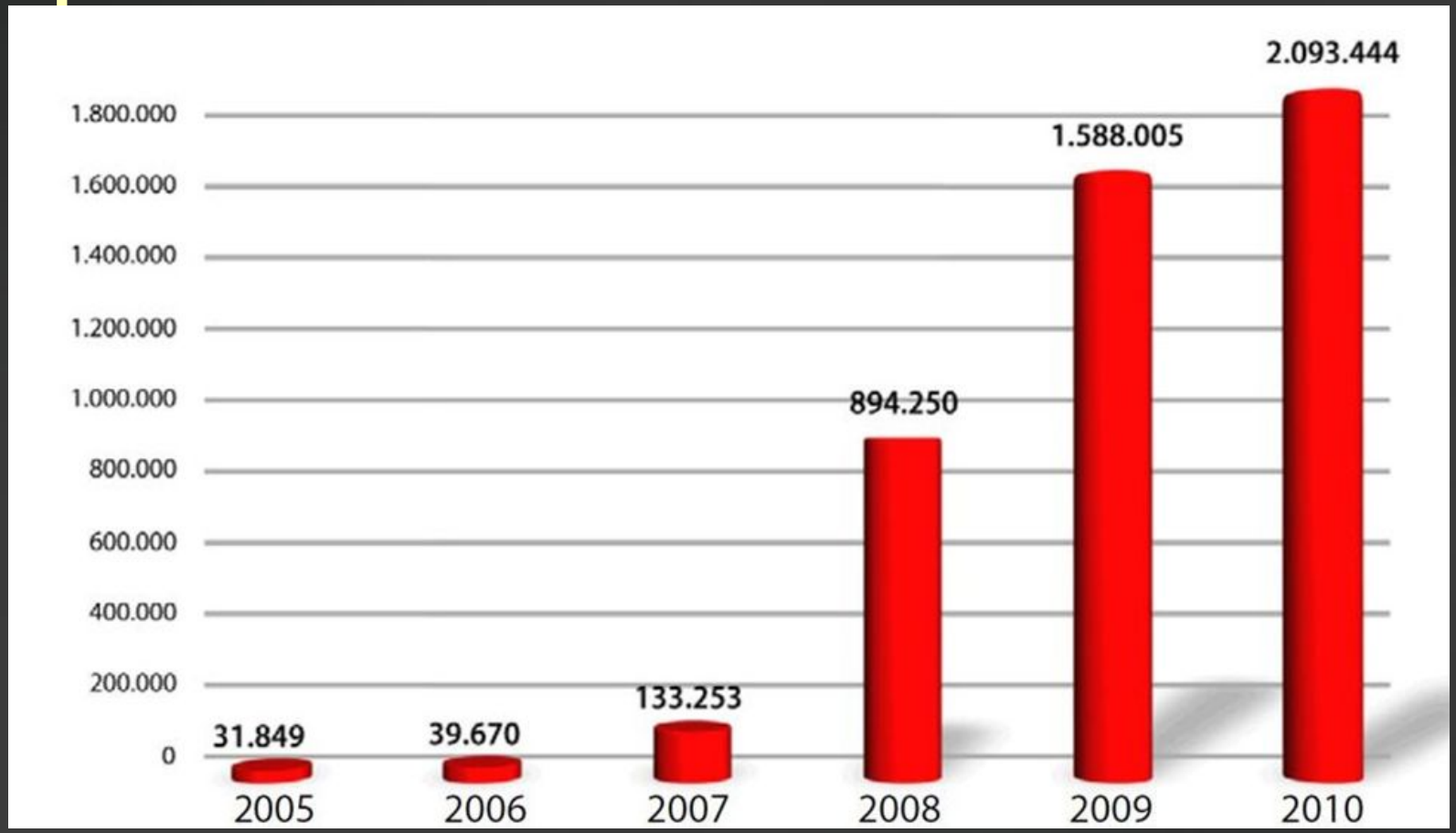
Предпосылки переноса безопасности в облака

- 200 000 000 сетевых атак блокируется ежемесячно
- 2 000 уязвимостей в приложениях обнаружено только в 2010 году
- 35 000 вредоносных программ появляется ежедневно
- 19 000 000 + новых вирусов появилось в 2010 году
- 30 000+ новых угроз появляется в день
- 3 500 новых сигнатур вирусов ежедневно

* *По данным Лаборатории Касперского*

Объем антивирусных обновлений (по версии лаборатории касперского)

Рост числа вирусов по версии компании G-Data



Данные AV-Test

- 20 000 000 образцов в 2010
- 12 000 000 в 2009

Вопросы

- Где хранить информацию о компьютерных угрозах?
- Как обеспечить мгновенную реакцию на них?
- Если проактивные технологии не эффективны…?

Ответ

- Облачная защита
- Сервисы репутации

Как было ранее?

- От пострадавшего пользователя лаборатория получала образец вредоносного файла и выпускала обновления к базе сигнатур вирусов вместе с рецептом по удалению заразы
- По мере роста числа угроз, производителям антивирусов пришлось максимально автоматизировать процесс анализа новых видов угроз, используя эвристические механизмы и даже встроить подобные механизмы в сами антивирусы.

Как было ранее?

- При этом частота обновлений увеличилась и выпуски стали ежедневными и даже ежечасными.
- Экспоненциальный рост числа новых угроз не оставляет этому подходу шанса.
- Антивирусные компании не в силах наращивать человеческие ресурсы такими же экспоненциальными темпами.
- Объем выпускаемых обновлений выходит за все разумные пределы.

Эвристические технологии

- Эвристические технологии – методики детектирования не на основе сигнатуры, а с использованием методов искусственного интеллекта, встраиваемого в антивирус.
- Лучшие примеры реализации эвристического анализа обеспечивают уровень обнаружения в пределах 50-70% для знакомых семейств вирусов и совершенно бессильны перед совершенно новыми видами атак.

Сегодня

- Распознавать угрозы необходимо непосредственно в распределенных центрах обработки данных антивирусной компании, а не только на компьютере конечного пользователя. Такой подход называется «облачным».
- Переход к облачным технологиям позволяет упростить архитектуру продукта, ведь теперь для каждого подозрительного ресурса предоставляется небольшое по объему обновление, индивидуально загружаемое из облака практически в реальном времени.

Сегодня

- По данным исследования, проведенного во втором квартале 2010 года компанией NSS Labs, время, необходимое антивирусным компаниям для блокирования web-угроз, составляет от 4,62 до 92,48 часа (http://nsslabs.com/host-malware-protection/q2-2010-endpoint-protection-product-group-test-report.html).
- Дальнейшее принципиальное увеличение максимальной скорости реакции на угрозы с помощью обычных антивирусных обновлений невозможно.

TREND MICRO SPN

Smart Protection Network

- Ключевой идеей этой системы была концепция “репутации”, то есть вынесения вердикта для ресурса (файла, сайта, сообщения электронной почты) только на основе накопленных ранее данных, без необходимости анализировать сам ресурс непосредственно в момент обращения к нему пользователя.
- На самом деле это единственный подход, который позволяет автоматически отражать неизвестные угрозы в автоматическом режиме.

Методы отслеживания репутации

- Формирование базы ресурсов, например сайтов, и отслеживание происходящих изменений.
- Если, например, сайт слишком часто меняет свой IP-адрес, то это типичный признак вредоносного сайта.
- Антивирус Trend Micro в реальном времени сверяется с SPN и блокируется доступ.

Базы репутации источников сообщений электронной почты и отдельных файлов

- SPN хранит базу репутации источников сообщений электронной почты, а также базу репутации отдельных файлов.
- Наличие всех трех баз, дает второй и самый изощренный способ выявления угроз.

Корреляция

- Суть метода в том, что используя информацию в одних базах наполняются другие.

Пример 1

- Рассмотрим сообщение электронной почты, которое приходит в ловушку для спама в TrendLabs с известного источника спама. Если к сообщению прикреплен исполняемый файл, то с него снимается контрольная сумма и она пополняет базу репутации файлов.
- Одновременно этот файл автоматически запускается в контролируемом окружении и выявляется, например, что он загружает из Интернета еще два каких-то исполняемых файла. Отметим, что именно такое поведение характерно для популярных последнее время троянов семейства Trojan.Downloader.
- Хеш-суммы загруженных файлов также помещаются в базу репутации файлов, а адреса, с которых производилась загрузка пополняют базу репутации сайтов.

Пример 2

- Если с серверов определенного провайдера рассылается подозрительно много спама, то и все сайты, которые размещены у данного провайдера получают низкую репутацию.
- Разумеется, что это не означает, что доступ к ним однозначно блокируется, но им оказывается более пристальное внимание.

Пример 3

- SPN учитывает обращение клиентов Trend Micro к ней для ее собственного пополнения.
- При выявлении спам-письма, IP-адрес отправителя помещается в базу на относительно короткий срок (в пределах нескольких часов). Такой осторожный подход призван застраховать от блокировки легитимных источников почты.
- Если же в течение этих нескольких часов большое количество клиентов Trend Micro обратиться к базе репутации электронной почты, чтобы свериться относительно репутации данного адреса, то это явный признак того, что адрес попал с базу не случайно.

Суть SPN

- Эта облачная инфраструктура позволяет отслеживать поведение вредоносных программ в масштабе всего интернета, а не непосредственно на компьютере жертвы.
- Это дает существенные преимущества перед современными угрозами, которые научились обманывать, как пользователя, так и защитное ПО, установленное у него на компьютере.

ИСПОЛЬЗОВАНИЕ ГИБРИДНОЙ ЗАЩИТЫ В KASPERSKY INTERNET SECURITY 2012

Антивирусное «облако» Kaspersky Security Network

- Эта облачная система безопасности была создана для максимально оперативного реагирования на новые угрозы в 2008 году и с тех пор является одной из ключевых технологий защиты ПК в продуктах «Лаборатории Касперского».
- При установке продукта Лаборатории Касперского пользователю явно предлагают согласиться на передачу данных о запускаемых программах в «облако». Эти данные полностью анонимны, но они позволяют определить новое вредоносное ПО и оповестить всех других пользователей буквально в течение нескольких минут.

Kaspersky Security Network

- Автоматический сбор данных о зловредах
- Автоматическая обработка информации
- Мгновенный доступ к информации об угрозах

Для чего это нужно?

- Быстрый ответ на новые угрозы
- Отсутствие необходимости хранить данные на компьютере
- Минимальная загрузка компьютера при «общении с облаком»

Окно ksn


KASPERSKY lab
INTERNET SECURITY 2012
online
Отчеты
Настройка
Назад
Kaspersky Security Network - это:
Сеть информационной безопасности, объединяющая пользователей во всем мире
Дополнительный уровень защиты
Оперативные данные о репутации программ
Оперативные данные о репутации веб-сайтов
Немедленная реакция на появление новых угроз
Узнать больше...
Статус: репутационные базы подключены.
Последняя синхронизация:
29.03.2011 07:55
За последние 24 часа:
Защищено пользователей: 1607250
Нейтрализовано угроз: 10053515
Справка
Поддержка
Личный кабинет
Управление лицензиями

Преимущества использования «облачной» технологии антивирусной защиты

- Высокая скорость реакции на угрозы, вплоть до десятков секунд
- Обладая практически неограниченными вычислительными ресурсами, «облако» позволяет производить параллельную обработку данных, то есть быстро выполнять исследование сложных угроз.
- При работе с «облаком» загрузка пользовательского компьютера минимальна, так как обмен информации с ним, как правило, осуществляется в фоновом режиме.

Как это работает?

- Основная задача антивируса заблокировать появление на компьютере вредоносных программ.
- К сожалению, на современном компьютере регулярно появляются новые программы. Даже если сам пользователь ничего не устанавливает, многие уже установленные программы (продукты компании Adobe, Apple, Google и т.д.) автоматически обновляют себя, загружая из Интернета свои новые версии.
- Это очень удобно для пользователя, но осложняет работу антивирусу. Ведь распространение нового вируса или троянской программы происходит сходно: в системе «вдруг» появляется новая программа.

Что произойдет, если программа все же оказалась вредоносной?

- Пользователи, попытавшиеся запустить ее в первые минуты атаки, будут защищены только с помощью поведенческого анализа, который способен выявить «подозрительную» активность.
- Все остальные участники KSN оперативно получат информацию о новой угрозе и будут предупреждены при попытке запуска соответствующего файла. Данные также поступят в распоряжение экспертов «Лаборатории Касперского» для последующего анализа.

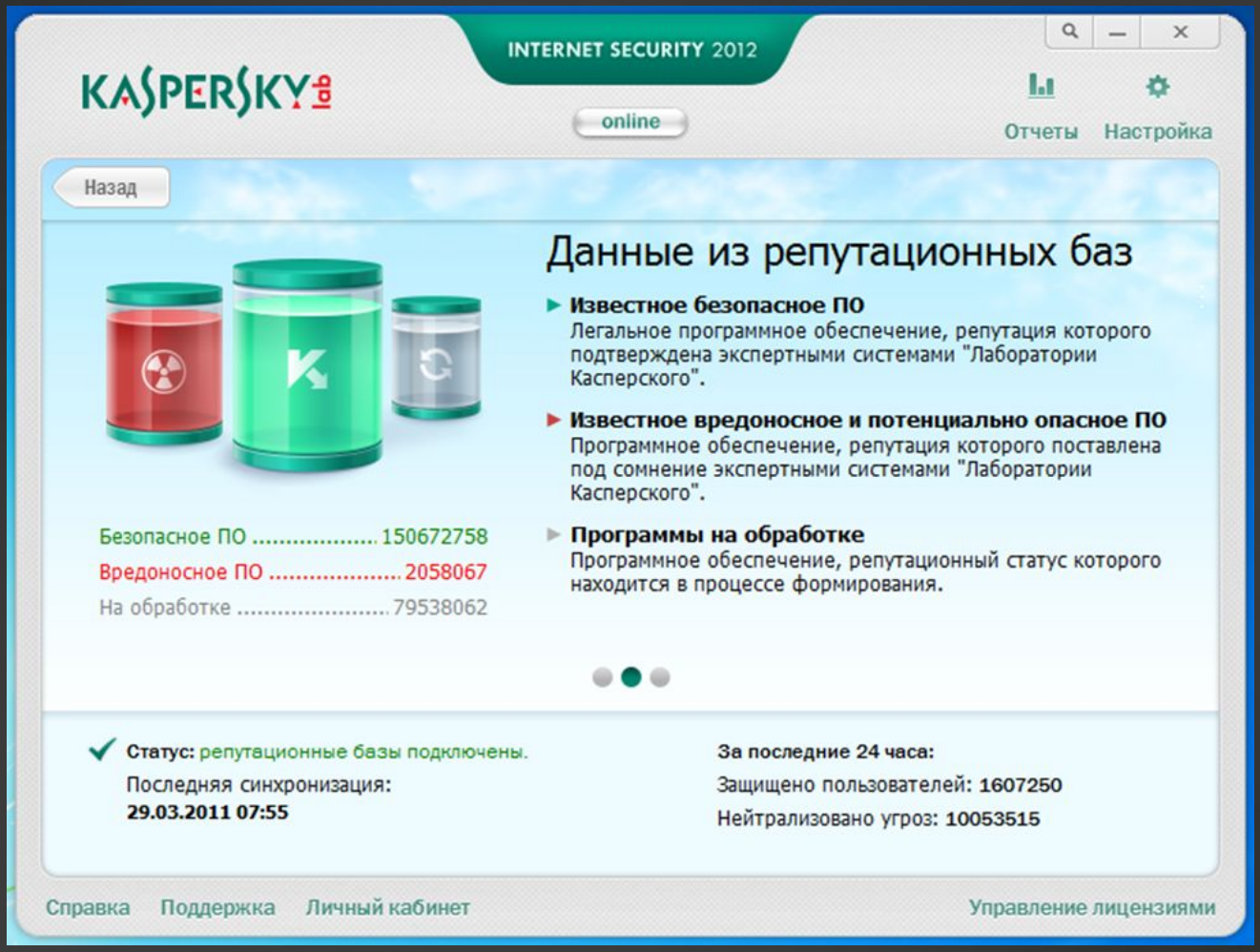
Как это работает?

- Такой подход принципиально отличается от традиционного. При традиционном обновлении антивирусных баз обратной связи от пользователя к серверу нет, поэтому антивирусная лаборатория не получает информацию о факте заражения, его источниках и распространении вредоносного ПО.

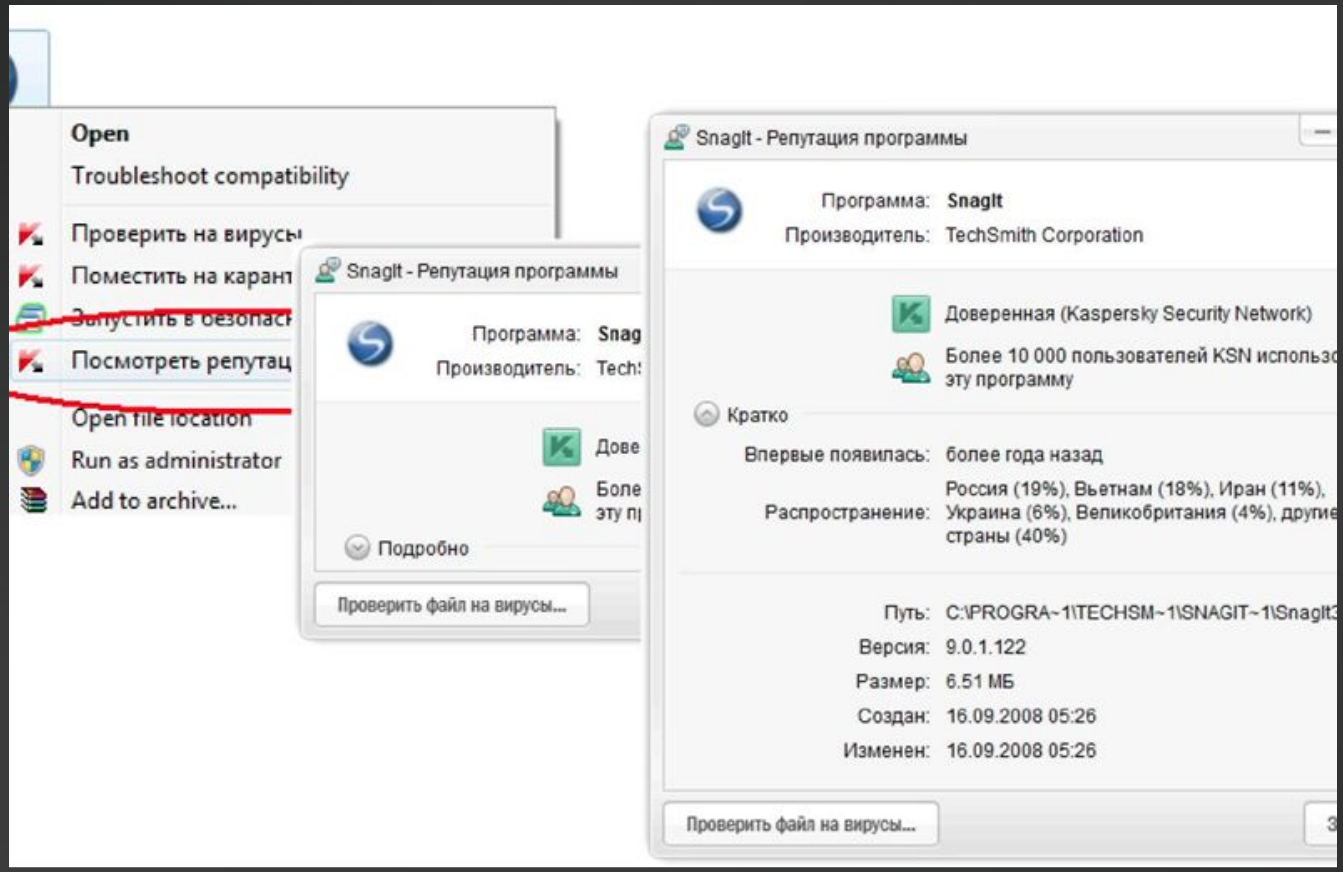
Как это работает?

- В лабораторию никогда не пересылается сам подозрительный файл, а только его свойства: хеш-функция, информация о поведении, источник появления и т.д.
- Таким образом, у пользователя не должно возникать никаких беспокойств по поводу утечки приватных данных.

Данные из репутационных баз



Проверка репутации программ



Причины недостаточности использования только «облачного» решения

- Чем быстрее пополняется «облачная» коллекция, тем более эффективную защиту оно может представить. Источники поступления в данном случае :
  - специальные вирусные ловушки, организованные специалистами антивирусных лабораторий
  - обмен экземплярами вредоносного кода между различными антивирусными компаниями
  - информация поступающая с компьютеров пользователей KSN.

Причины недостаточности использования только «облачного» решения

- В случае если ваш ПК не подключен к Интернет, «облачная»защита просто не работает. Но ведь источники заражения (локальная сеть, USB-носители и т.п.) никуда не исчезают, увы. Сегодня по данным «Лаборатории Касперского» при наличии интернет соединения с помощью облачных технологий отсекается 30% вирусных заражений. А остальные – только локальным продуктом.

Вывод

- **Продукт, обеспечивающий антивирусную защиту на компьютере пользователя необходим, потому что:**
  - Он обеспечивает защиту при отсутствии подключения к Интернет
  - В случае если заражение все же произошло, вылечить зараженный ПК через Интернет часто невозможно, так как вредоносное ПО может просто блокировать соединение с Интернет.

ИСПОЛЬЗОВАНИЕ ФИЛЬТРА SMARTSCREEN

Результаты анализа SmartScreen Filter

- Каждая четырнадцатая программа, загружаемая пользователями Windows, является вредоносной, однако около 5% пользователей игнорируют предупреждения и скачивают опасные приложения.
- SmartScreen блокирует ежечасно более 125 тыс. потенциально небезопасных сайтов и программ.

Три способа защиты от мошеннических и вредоносных узлов

- Сравнение адреса посещаемого сайта со списком известных сайтов. Если сайт найден в этом списке, больше проверок не производится.
- Анализ сайта на предмет наличия признаков, характерных для мошеннических сайтов.
- Отправка адреса сайта, на который пользователь собирается зайти, онлайн-службе Microsoft, которая ищет сайт в списке фишинговых и вредоносных сайтов.

Как работает SmartScreen

- Работа фильтра SmartScreen основывается на службе Microsoft URL Reputation Service (URS), осуществляющей круглосуточную поддержку. Если фильтр SmartScreen включен, то он просматривает локальный список известных разрешенных узлов и отправляет адрес URL узла службе URS для проверки.
- Во избежание задержек обращения к URS производятся асинхронно, так что на работе пользователя это не отражается.
- Чтобы уменьшить сетевой трафик, на клиентском компьютере хранится зашифрованный файл со списком в несколько тысяч наиболее посещаемых узлов; все включенные в этот список узлы не подвергаются проверке фильтром SmartScreen.

Как работает SmartScreen

- В фильтре SmartScreen применяется механизм локального кэширования адресов URL, позволяющий сохранять ранее полученные рейтинги узлов и избежать лишних обращений по сети. Один из способов выявления потенциально подставных узлов, применяемый службой URS, — сбор отзывов пользователей о ранее неизвестных узлах.
- Для защиты от фишинга и эксплойтов фильтр SmartScreen исследует строку URL целиком, а не подмножество адресов URL, на которые заходил пользователь.
- **Службе URS могут быть переданы личные сведения, поскольку иногда они находятся в самой строке URL.**

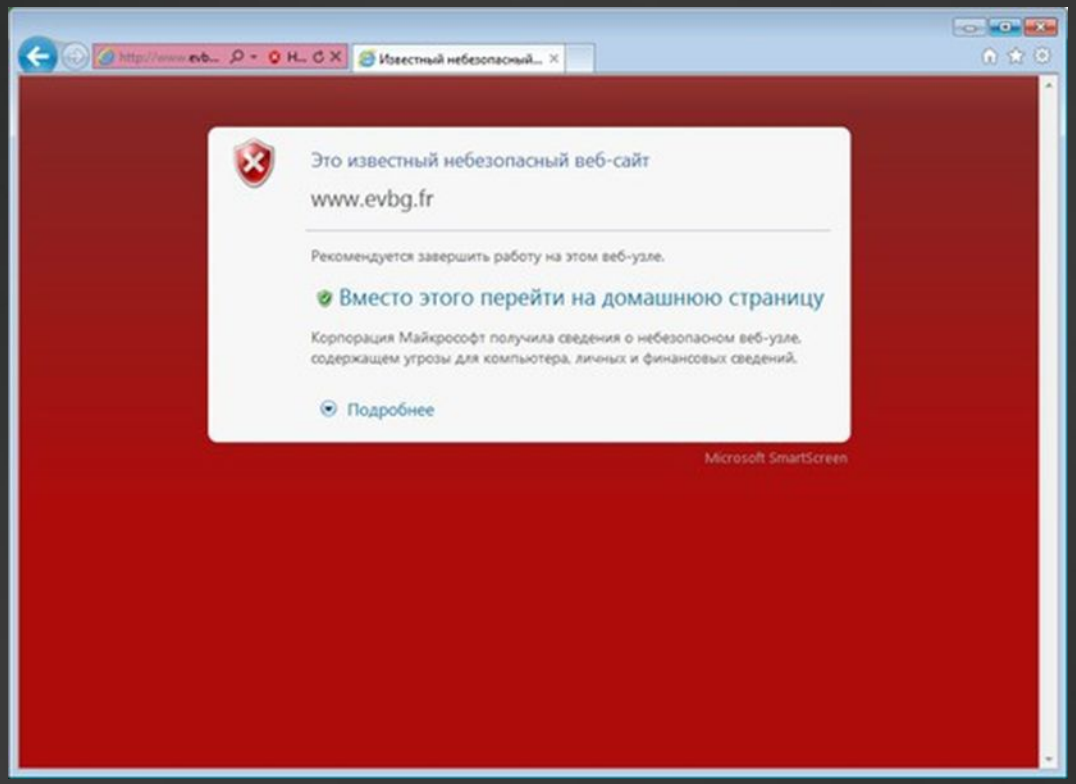
Включение/отключение

- Фильтр SmartScreen можно включать или отключать избирательно для каждой зоны безопасности, но только в том случае, когда эта функция включена глобально.

Включение/отключение

- По умолчанию фильтр SmartScreen включен для всех зон, кроме местной интрасети. Если вы захотите исключить некоторые узлы из списка проверяемых фильтром SmartScreen, но не отключать при этом фильтр полностью, то необходимо включить фильтр глобально, а затем отключить фильтрацию только для зоны «Надежные узлы», после чего конкретные узлы добавить в эту зону.

Предупреждение, выдаваемое фильтром SmartScreen в IE9

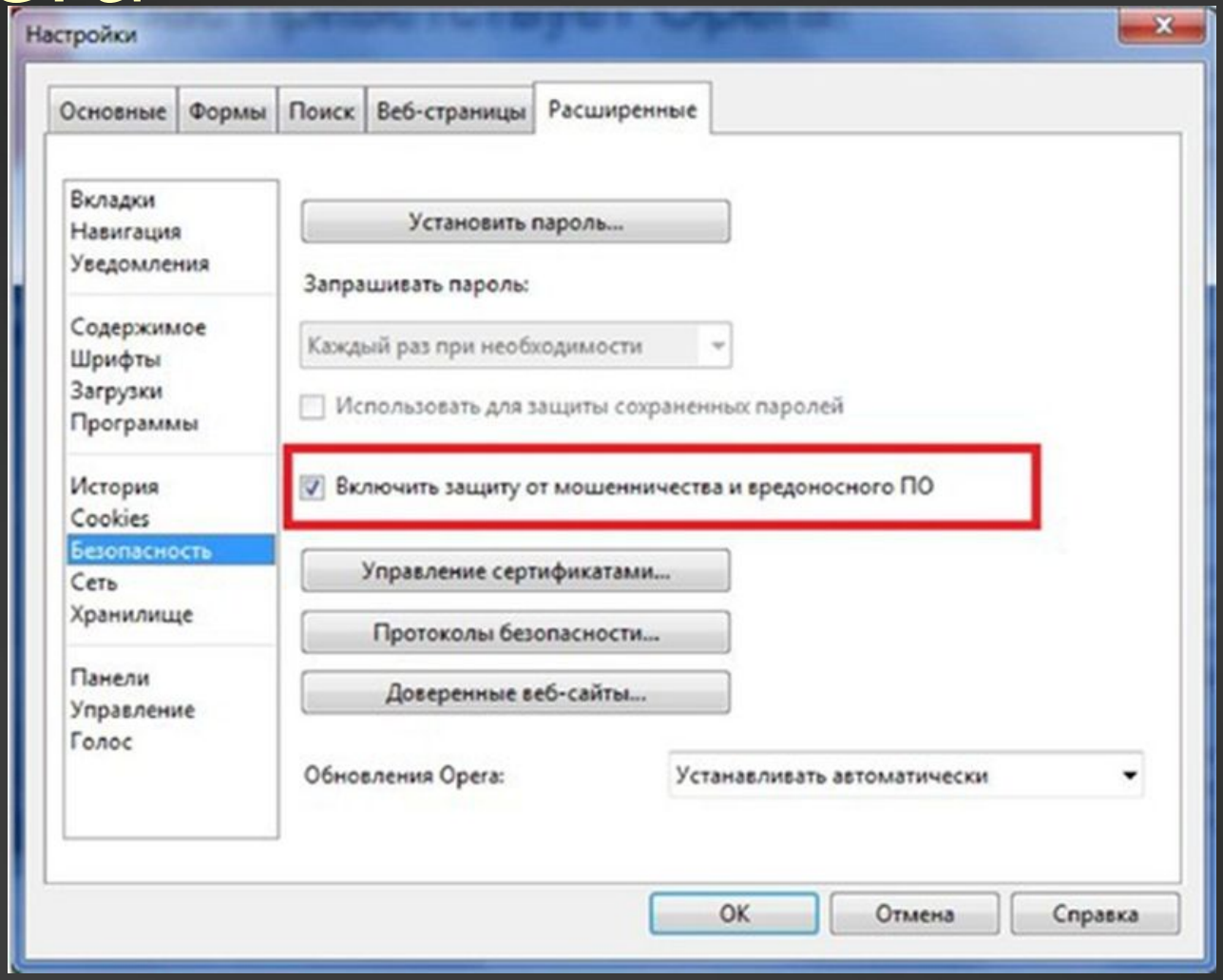


АНТИФИШИНГОВАЯ ЗАЩИТА В OPERA

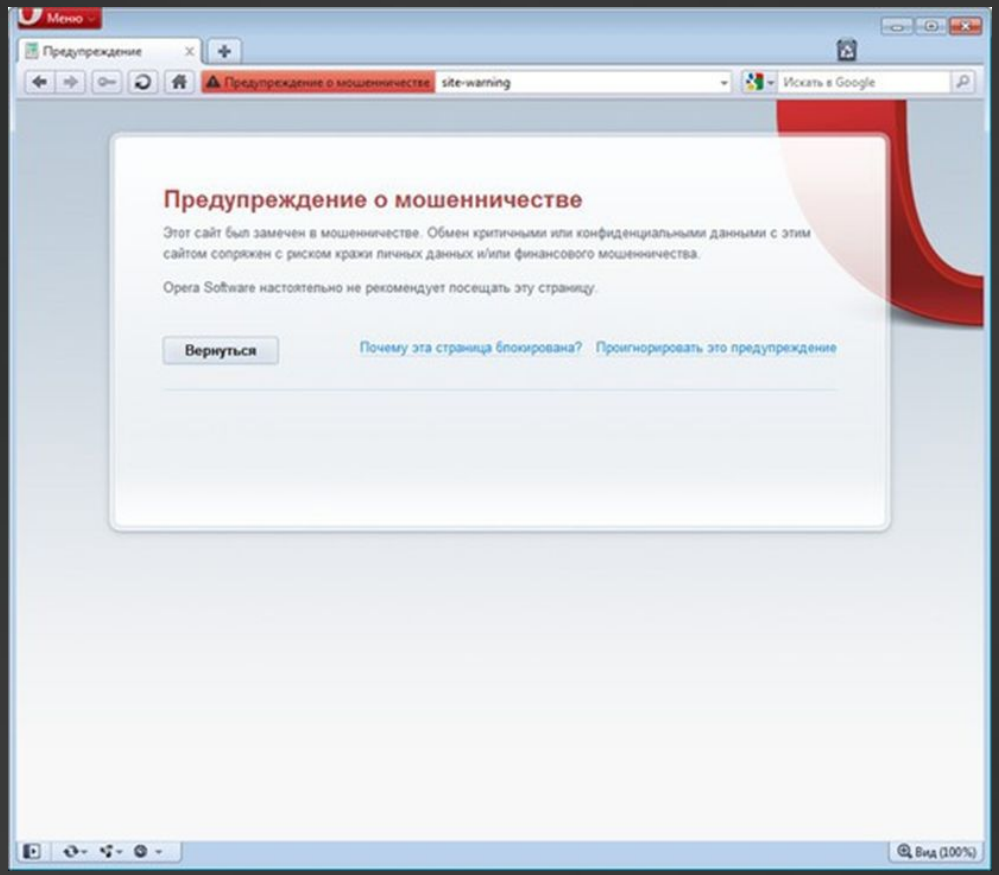
Антифишинговая защита в Opera

- Для защиты от фишинга используется функция «Защита от мошенничества» (Fraud and Malware Protection).
- В начале каждого сеанса с конкретным веб-сайтом она проверяет адрес, используя шифрованный канал (https): передается имя домена и адрес запрашиваемой страницы на сервер, где ищет его в черных списках фишинговых ссылок, формируемых Netcraft (www.netcraft.com) и PhishTank (www.phishtank.com), а также в списках сайтов с вредоносным ПО, которые ведет «Яндекс».
- Opera Fraud and Malware Protection server не отсылает любую идентифицирующую информацию.

Антифишинговый фильтр в Opera



Предупреждение о мошенничестве в Opera



ЗАЩИТА ОТ ФИШИНГА И ВРЕДОНОСНОГО ПО В GOOGLE CHROME

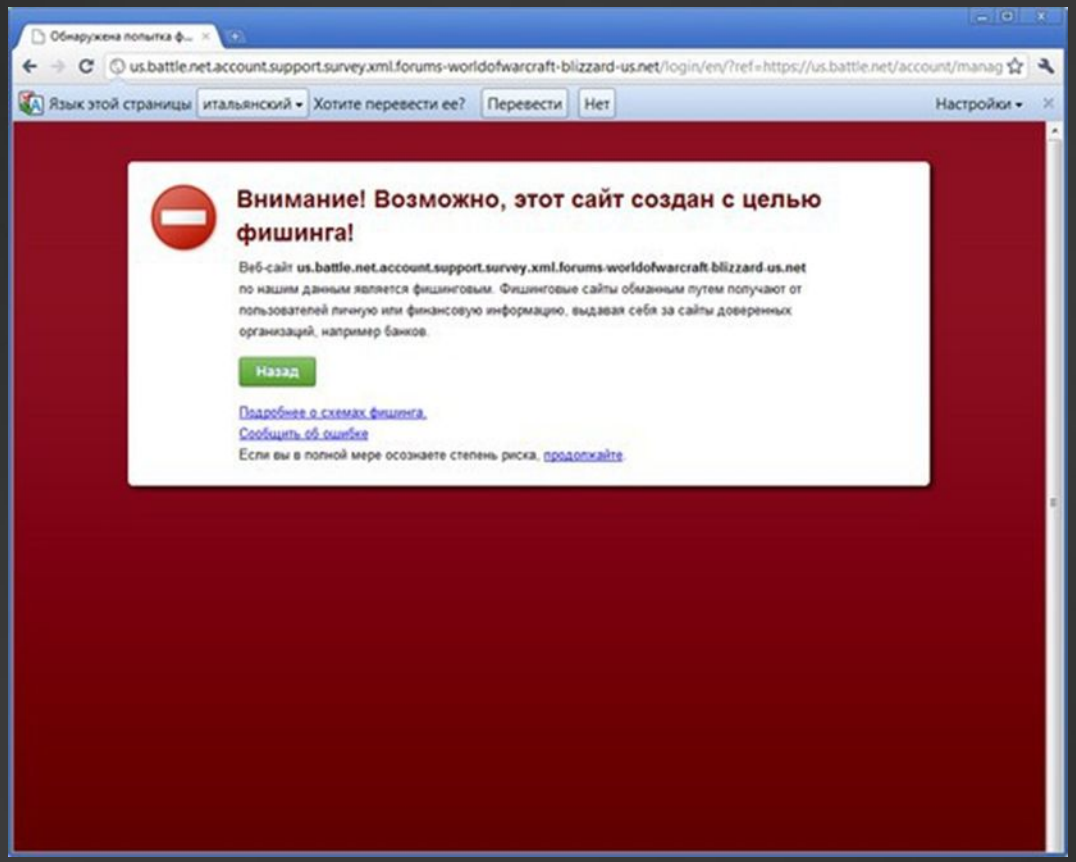
Принцип работы

- В браузер загружается список с информацией о сайтах, которые могут содержать вредоносное ПО или подозреваются в фишинге. Этот список не содержит полные адреса URL каждого подозрительного сайта.
- Вместо этого каждый URL хэшируется и разделяется на фрагменты. Только часть каждого хэшируемого URL включается в список в браузере.

Принцип работы

- При работе в Интернете браузер создает хэшированные версии посещаемых URL и проверяет их в соответствии со списком.
- Если адрес посещаемого сайта соответствует хэшированному фрагменту URL в списке, браузер свяжется с серверами Google и запросит полный список (а не только фрагменты) хэшированных URL подозрительных страниц.
- Затем компьютер определит, является ли сайт подозрительным, и выведет соответствующее предупреждение.

Предупреждение о фишинговом сайте в Google Chrome

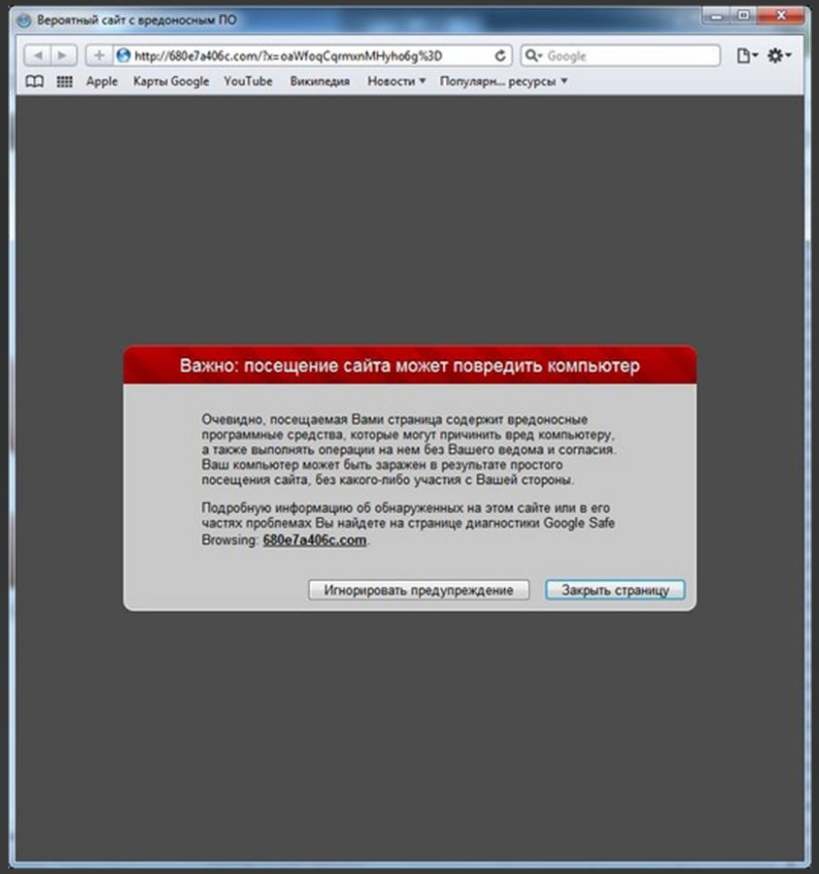


ЗАЩИТА ОТ ФИШИНГА И ВРЕДОНОСНОГО ПО В SAFARI

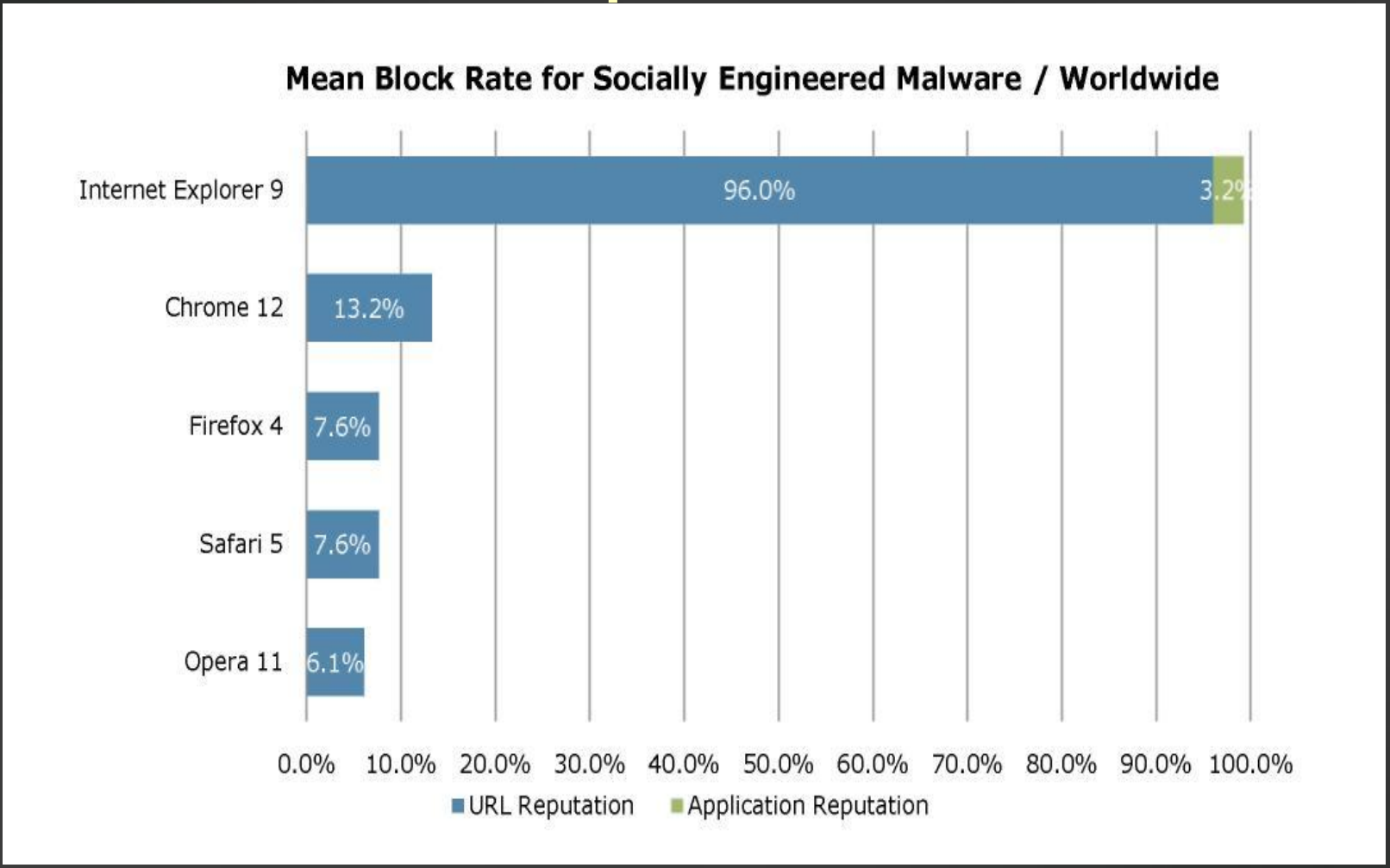
Принцип работы

- Как только пользователь пытается открыть подозрительную страницу в Safari, браузер соединяется с Google и запрашивает информацию из двух основных баз Google: базы фишинговых ссылок и базы ссылок вредоносного ПО. При наличии совпадения пользователь должен увидеть страницу с предупреждением.

Предупреждение о переходе на сайт, содержащий вредоносное ПО, в браузере Safari



Результаты тестирования NSS Labs за 3-й квартал 2011 года



Спасибо за внимание!
Вопросы?

Безмалый В.Ф.
MVP Consumer Security
Microsoft Security Trusted Advisor
http://bezmaly.wordpress.com
vladb@windowslive.com


TechDays.ru