Служба репутаций

Владимир Безмалый

В наше время написание вирусов стало видом бизнеса, своего рода отраслью промышленности. Времена хакеров-одиночек давно прошли. Нравится нам или нет, но борьба с вирусами — это борьба с международным преступным сообществом. Основная цель вирусописателей сегодня — деньги. Уже давно у них появилось разделение труда: один находит уязвимые места, другой реализует их в виде тех или иных законченных решений, третий продает эти решения на бирже, четвертый покупает и применяет, а пятый все это оплачивает...

Обратимся к фактам

Специалисты лаборатории G Data Security Labs в сентябре 2011 года обнаружили на подпольном форуме распродажу сетей дистанционно управляемых злоумышленниками компьютеров — так называемых ботов, которые в случае активации могут вызвать массивную волну вредоносного кода по всему Интернету. «Бот-конструктор» Aldi Bot продавался в конце августа по цене всего 10 евро. Часть вредоносного кода очень напоминает знаменитую сеть ZeuS. Суть предложения: программа-конструктор + бот + обновления + помощь в установке = 10 евро. Более того, недавно цена уже достигла 5 евро.

Для новичков в организации хакерских атак, которые не имеют ни малейшего представления о том, как работают средства атаки, проводится специальный «курс молодого бойца». Более того, заботливый автор продукта также использует TeamViewer, чтобы еще лучше подготовить своих покупателей к атаке. Это очень напоминает своеобразную службу клиентской поддержки для хакеров. А теперь ближе к делу: наличие такого дешевого вредоносного кода на рынке делает организацию атаки типа DDoS развлечением и легким способом заработать деньги. Юные хакеры могут купить программу для создания бот-сети вместе с обновлениями и технической поддержкой на деньги, выданные родителями на карманные расходы. Таким образом, становится очевидной причина стремительного роста числа вредоносных программ.

Обратимся к истории

С момента зарождения антивирусной индустрии сложился понятный механизм обеспечения защиты, когда от пострадавшего пользователя или из другого источника лаборатория получала образец вредоносного файла и после всестороннего анализа выпускала обновления к базе сигнатур вирусов вместе с рецептом по удалению заразы. Все клиенты загружали это обновление и получали актуальную защиту. Разумеется, кто-то заражался раньше, чем получал обновление, но таких было довольно мало. 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. При этом частота обновлений увеличилась и выпуски стали ежедневными и даже ежечасными. Несмотря на успехи антивирусных компаний в описанных способах ускорения выпуска обновлений, очевидно, что экспоненциальный рост числа новых угроз не оставляет этому подходу шанса. С одной стороны, антивирусные компании не в силах наращивать человеческие ресурсы такими же экспоненциальными темпами. С другой стороны, объем выпускаемых обновлений превышает все разумные пределы.

Одно время в индустрии безопасности бытовало мнение, что описанную проблему раз и навсегда решат так называемые эвристические технологии, то есть методики детектирования не на основе сигнатуры, а с использованием методов искусственного интеллекта, встраиваемого в антивирус. Эти технологии получили широкое распространение, но проблемы не решили. Лучшие примеры реализации эвристического анализа обеспечивают уровень обнаружения в пределах 50–70% для знакомых семейств вирусов и совершенно бессильны перед новыми видами атак.

В настоящий момент уже сформировалась тенденция распознавать угрозы непосредственно в распределенных центрах обработки данных антивирусной компании, а не только на компьютере конечного пользователя. Такой перенос центра тяжести технологии в Интернете называется «облачным».

Переход к «облачным» технологиям позволяет упростить архитектуру продукта, который пользователь ставит на свой компьютер, ведь теперь для каждого подозрительного ресурса предоставляется небольшое по объему обновление, индивидуально загружаемое из «облака» практически в реальном времени. Разумеется, разработанные технологии существенно сложнее, ведь многие процессы в компьютере требуют меньшего времени реакции, чем интервал получения подобных обновлений. Кроме того, необходимо обеспечить защиту в тот момент, когда компьютер вообще не подключен к Интернету. Тем не менее «облачные» технологии являются ключом к обеспечению безопасности не самых мощных компьюте-

ров, таких как нетбуки, планшеты и смартфоны.

Что такое служба репутации?

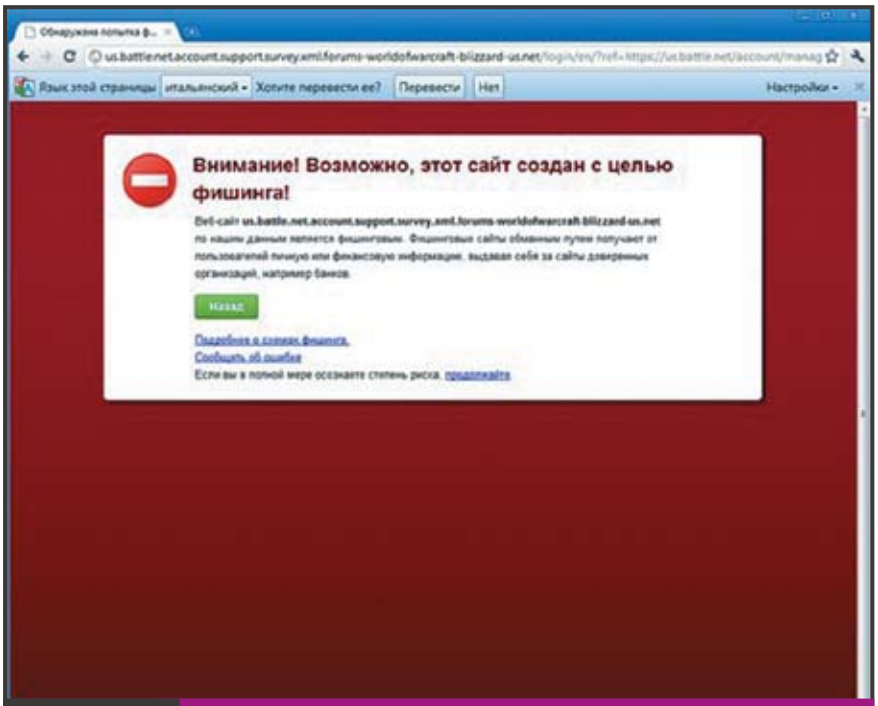
Службы репутации показывают надежность того или иного источника (почта, Интернет), репутацию того или иного программного обеспечения. При этом вычисление репутации производится на серверах соответствующего производителя в Интернете.

Рассматривая службы репутации, стоит различать «облачные» службы, применяемые сегодня в браузерах Google Chrome, Safari, Opera, Internet Explorer, и антивирусные «облачные» службы репутации. В браузере Firefox не реализована «облачная» служба репутации, обработка репутации происходит на компьютере пользователя (проводится поиск в базах, загружаемых на компьютер пользователя). Рассмотрим, как работают службы репутации в различных браузерах.

Google Chrome

Функция безопасного просмотра Google Chrome, отвечающая за обнаружение фишинга и вредоносных программ, включена по умолчанию. При попытке посещения сайта, подозреваемого в фишинге или распространении вредоносных программ, браузер выдает предупреждение (см. экран 1).

Функция безопасного просмотра защищает нас от фишинга и вредоносных программ двумя способами. Во-первых, Google загружает в браузер информацию о сайтах, которые могут содержать вредоносные программы или подозреваются в фишинге. Списки подозрительных сайтов, позволяющие сэкономить место и предотвратить выдачу URL на небезопасные сайты, обычно содержат достаточно информации, чтобы определить, что сайт содержит вредоносные программы или создан с целью фишинга, но недостаточно, чтобы с уверенностью сказать, какую именно из этих двух угроз он представляет. Если URL просматриваемого сайта совпадает с записью в списке, браузер запрашивает дополнительную информацию с серверов Google для принятия решения. Информация, которую отправляет браузер, не позволяет компании Google установить, какой именно сайт вы просматриваете (отправляются только первые 32 бит хэша SHA-256 копии URL). Если компьютер расценит сайт как опасный, будет выдано предупреждение.



Экран 1 Предупреждение о фишинговом сайте в Google Chrome

В случае если компьютер обращается в Google для запроса информации о конкретном фрагменте URL или для обновления списка, будет отправлен стандартный набор данных, в том числе ваш IP-адрес, а иногда и файл cookie. На основе этих данных невозможно установить личность. Кроме того, эти данные хранятся в Google всего несколько недель. Вся информация, полученная таким образом, защищается в соответствии со стандартными условиями политики конфиденциальности Google.

Во-вторых, безопасный просмотр защищает от целевого фишинга (так называемого spear-phishing), при котором сайт может быть еще не зарегистрирован в списках опасных сайтов Google. Для этого Chrome анализирует содержание сайта и, если оно кажется подозрительным, выдает предупреждение.

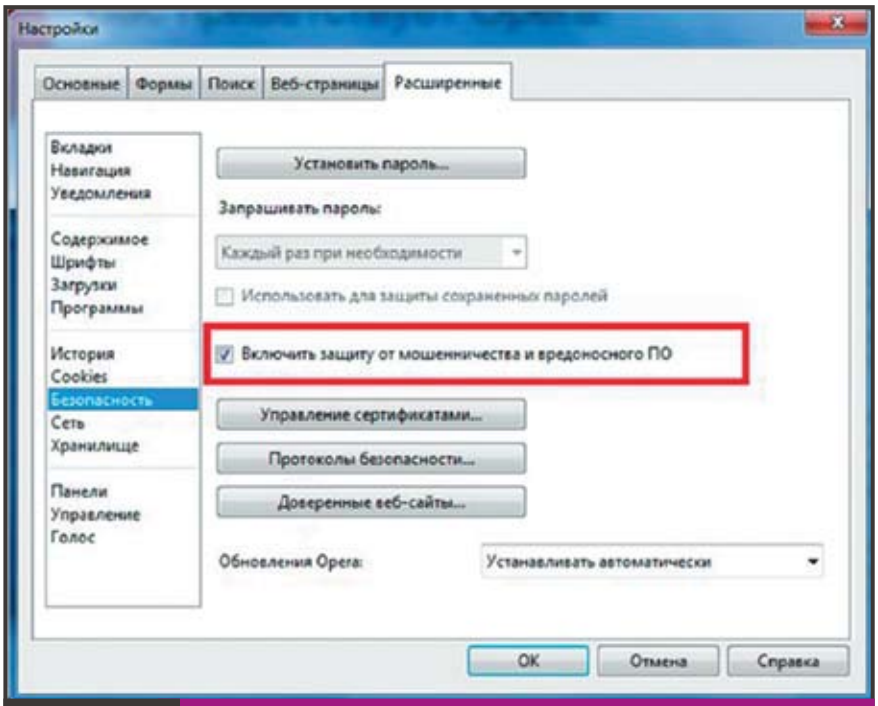
Кроме того, если вы решили предоставлять Google статистику об использовании и зашли на сайт, который может оказаться опасным, в Google отправляются и некоторые другие данные, в том числе полный URL посещаемой страницы, заголовок referer, отправленный на нее, и URL, совпавший с одним из адресов в списке вредоносных программ функции безопасного просмотра Google.

Отключить эту функцию можно в меню «Параметры — Расширенные — Конфиденциальность». Для этого достаточно снять флажок «Включить защиту от фишинга и вредоносных программ».

При включенной защите от фишинга и вредоносных программ отображаются сообщения, приведенные в таблице.

Антифишинговая защита в Opera

В этом браузере для защиты от фишинга используется функция защиты от мошенничества (Fraud and Malware Protection), включенная по умолчанию (экран 2). В начале каждого сеанса с конкретным веб-сайтом она проверяет адрес, используя шифрованный канал (https): передает имя домена и адрес запрашиваемой страницы на специальный сер-



Экран 2 Антифишинговый фильтр в Opera

Таблица Сообщения Google Chrome

Сообщение	Значение
Внимание! Обнаружена проблема	Это сообщение отображается для сайтов, которые Google Chrome определяет как потенциально содержащие вредоносные программы
Внимание! Возможно, этот сайт создан с целью фишинга	Это сообщение появляется, когда Google Chrome обнаруживает, что посещаемый вами сайт подозревается в фишинге

вер, где ищет его в черных списках фишинговых ссылок, формируемых Netcraft (www.netcraft.com) и PhishTank (www.phishtank.com), а также в списках сайтов с вредоносными программами, которые ведет «Яндекс».

Если доменное имя совпадет с именем из черного списка, сервер Fraud and Malware Protection возвратит браузеру документ XML, в котором будет описана проблема (фишинг или вредоносные программы).

При этом необходимо учесть следующее.

- Opera Fraud and Malware Protection server не сохраняет IP-адрес пользователя или любую другую идентифицирующую его информацию. Никакая сессионная информация, включая cookies, не сохраняется.
- В любое время можно отключить функцию защиты от мошенничества в меню «Настройки — Расширенные (Crtl-F12) — Безопасность».

Если веб-сайт найден в черном списке, в браузере откроется страница с предупреждением. Пользователю придется решить, посещать эту подозрительную страницу или вернуться на домашнюю. Механизм защиты от мошенничества не оказывает никакого воздействия на скорость открытия веб-страниц.

Safari

По умолчанию модуль защиты от фишинга в этом браузере включен. Для поиска фишинговых сайтов он использует технологии Google. 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 вредоносных программ. При обнаружении совпадения пользователь должен увидеть страницу с предупреждением (экран 3).

Фильтр SmartScreen в Internet Explorer 9

Начиная с Internet Explorer 8 в состав IE входит фильтр SmartScreen — набор технологий, предназначенный для защиты пользователей от возможных интернет-угроз, в том числе с использованием методов социальной инженерии. Базируется SmartScreen на технологии фишингового фильтра и предназначен для защиты пользователей от известных вредоносных сайтов. Кроме того, данный фильтр включает защиту от ClickJacking, технологии, применяемой для перехвата нажатий клавиш, искажения веб-страниц и т.д. По умолчанию он включен.

Фильтр SmartScreen в Internet Explorer 9 использует сразу несколько технологий. В первую очередь происходит сравнение адреса посещаемого сайта со списком известных мошеннических и вредоносных сайтов. Если сайт есть в этом списке, больше проверок не производится. В противном случае он анализируется на предмет наличия признаков, характерных для мошеннических сайтов. Также возможна отправка адреса того сайта, куда пользователь собирается зайти, онлайн-службе Microsoft, которая ищет его в списке фишинговых и вредоносных сайтов. Причем доступ к онлайн-службе производится асинхронно по SSL-соединению, так что это не сказывается на скорости загрузки страниц. Однако обращение к данной службе пользователь может запретить.

Чтобы уменьшить сетевой трафик, на клиентском компьютере хранится зашифрованный DAT-файл со списком тысяч наиболее посещаемых узлов; все включенные в этот список сайты не подвергаются проверке фильтром SmartScreen.

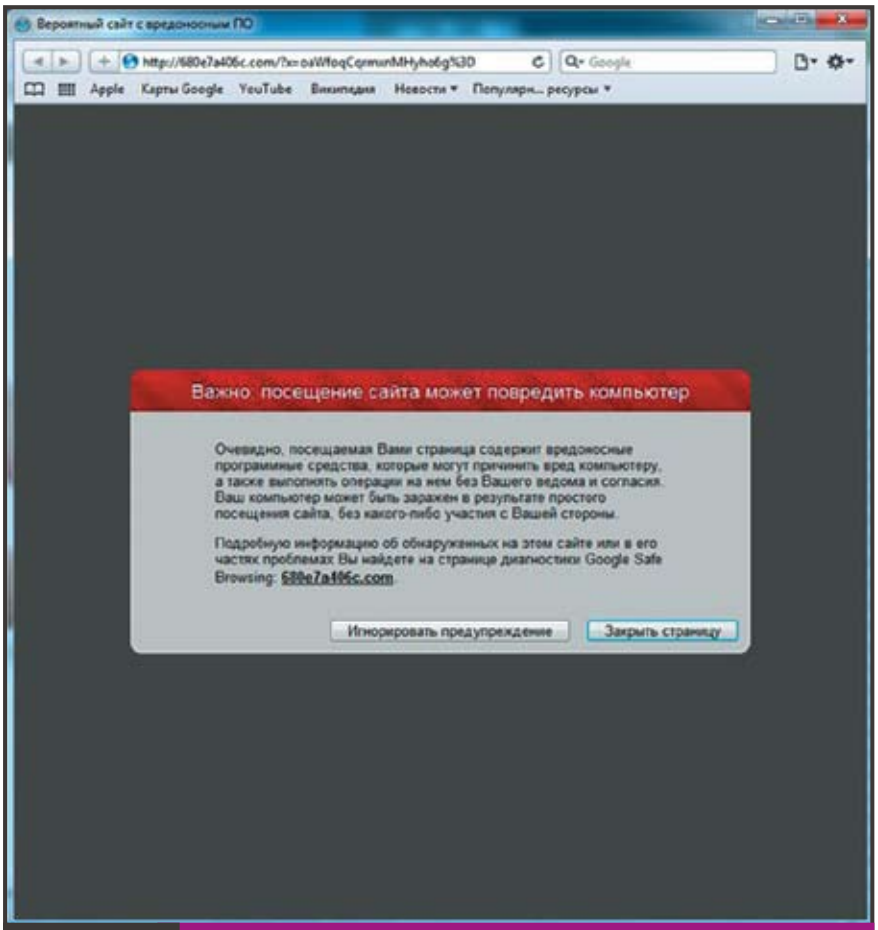
Для защиты от фишинга и вредоносных программ фильтр SmartScreen исследует строку URL целиком, а не подмножество адре-

сов URL, на которые заходил пользователь, а значит, службе URL Reputation Service (URS) могут быть переданы личные сведения, поскольку иногда они находятся в самой строке URL. Вместе с тем необходимо добавить, что в состав SmartScreen входит и проверка репутации загружаемых файлов Application Reputation Service (ARS)

При загрузке программы в IE 9 идентификатор файла и издателя приложения (если оно подписано цифровой подписью) отправляются на проверку с помощью новой услуги репутации приложений в «облаке». Если программа имеет репутацию, то предупреждение отсутствует. Если же файл будет загружаться с вредоносного сайта, IE 9 блокирует загрузку, так же как и IE 8. Однако, если файл не имеет данных о репутации, IE покажет это в строке уведомления и менеджере загрузки, что позволит принять обоснованное решение о доверии к этому файлу.

Фильтр SmartScreen в Internet Explorer 9 предупреждает пользователя о подозрительных или уже известных мошеннических веб-узлах. При этом фильтр проводит анализ содержимого соответствующего сайта, а также использует сеть источников данных для определения степени надежности сайта. Фильтр SmartScreen сочетает анализ веб-страниц на стороне клиента на предмет обнаружения подозрительного поведения с онлайн-службой, доступ к которой пользователь разрешает или запрещает. При этом реализуется три способа защиты от мошеннических и вредоносных узлов.

1. Сравнение адреса посещаемого сайта со списком известных сайтов. Если сайт найден в этом списке, больше проверок не производится.
2. Анализ сайта на предмет наличия признаков, характерных для мошеннических сайтов.
3. Отправка адреса сайта, на который пользователь собирается зайти, онлайн-службе Microsoft, которая ищет сайт в списке фишинговых и вредоносных сайтов. При этом доступ к онлайн-службе производится асинхронно по SSL-соединению, так что это не сказывается на скорости загрузки страниц.



Экран 3 Предупреждение о переходе на сайт, содержащий вредоносные программы

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 DAT-файл со списком тысяч наиболее посещаемых узлов; все включенные в этот список узлы не подвергаются проверке фильтром SmartScreen. В фильтре SmartScreen также применяется механизм локального кэширования адресов URL, позволяющий сохранять ранее полученные рейтинги узлов и избежать лишних обращений по сети. Один из способов выявления подставных узлов, применяемый службой URS, — сбор отзывов пользователей о ранее неизвестных узлах. Пользователь может решить, следует ли отправлять информацию об узле, который вызывает у него подозрения.

Для защиты от фишинга и вредоносных программ фильтр SmartScreen исследует строку URL целиком, а не подмножество адресов URL, на которые заходил пользователь. Учтите, что службе URS могут быть переданы личные сведения, поскольку иногда они находятся в самой строке URL.

Фильтр SmartScreen можно включать или отключать избирательно для каждой зоны безопасности, но только в том случае, когда эта функция включена глобально. 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, необходимо включить фильтр глобально, а затем отключить фильтрацию только для зоны «Надежные узлы», после чего конкретные

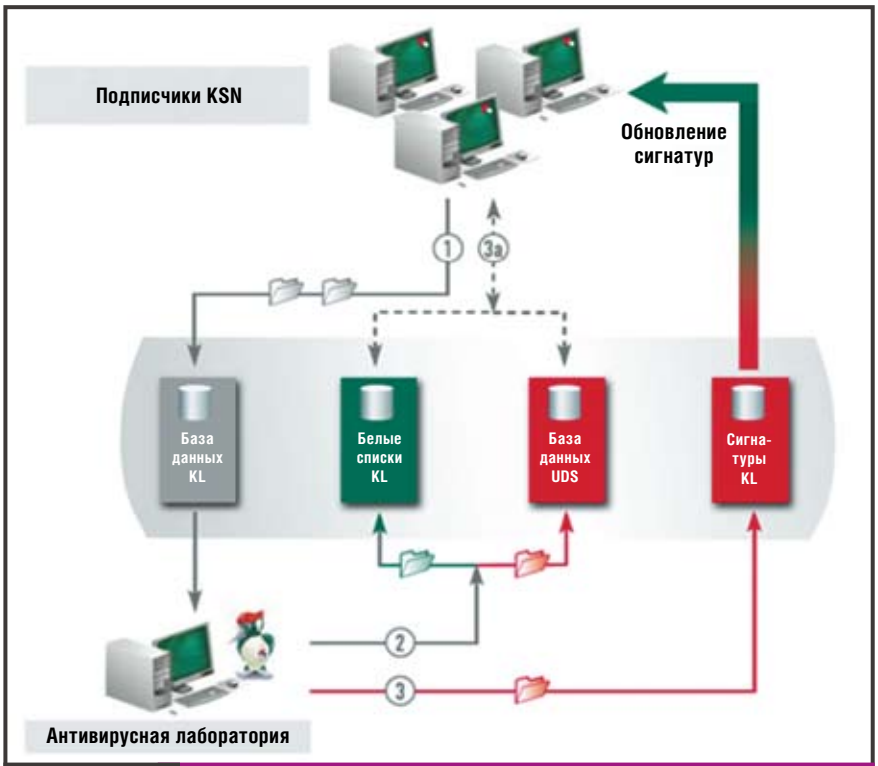


Рисунок Схема работы KSN

узлы добавить в эту зону. Для того чтобы пользователи в организации не могли отключить фильтр SmartScreen, необходимо применить групповую политику.

Службы репутаций в антивирусах

Kaspersky Security Network

Составными частями Kaspersky Security Network (KSN) являются несколько подсистем:

- географически распределенный мониторинг актуальных угроз на компьютерах пользователей;
- мгновенная доставка собранных данных на серверы «Лаборатории Касперского»;
- анализ полученной информации;
- разработка и применение мер защиты от новых угроз.

При помощи KSN автоматически собирается информация о попытках заражения, подозрительных файлах, загруженных на компьютеры пользователей, независимо от их источника (веб-сайты, письма, одноранговые сети и т. д.). Сеть Kaspersky Security Network создана для сбора и передачи информации о попытках заражения. Собранная информация отправляется экспертам «Лаборатории Касперского».

Информация о попытках заражения передается на серверы «Лаборатории Касперского», что обеспечивает быструю и надежную идентификацию программного обеспечения, как вредоносного, так и легитимного. Заключение о безопасности программы (ее репутации) выносится на основании цифровой подписи, удостоверяющей ее происхождение и гарантирующей целостность, а также ряда других признаков. Программа, признанная безопасной, включается в список доверенных приложений.

В случае если программа признана вредоносной, данные о ней поступают в Urgent Detection System (UDS), и эта информация становится доступной пользователям «Лаборатории Касперского» еще до создания соответствующей сигнатуры и включения ее в обновления антивирусных баз. Легитимные файлы вносятся в белые списки (Whitelisting). На рисунке показаны основные принципы взаимодействия KSN с компьютерами пользователей.

По завершении анализа новой вредоносной программы ее сигнатура вносится в соответствующие антивирусные базы. Кроме белых списков, в KSN используется технология Wisdom of the Crowd (WoC), предоставляющая информацию о популярности программы и ее репутации среди пользователей KSN.

Помимо этого, последние версии продуктов «Лаборатории Касперского» позволяют получать данные глобальных рейтингов безопасности (GSR) непосредственно из «облака». Рейтинг (GSR) каждой программы рассчитывается с помощью специального алгоритма и набора репутационных данных.

Таким образом, в Kaspersky Security Network используется сочетание сигнатурных и эвристических методов детектирования вредоносных программ, технологии контроля программ с использованием белых и черных списков и репутационных служб (WoC и GSR).

Trend Micro Smart Protection Network (SPN)

Служба репутаций в Trend Micro включает следующие технологии:

- Web Reputation;
- Email Reputation;
- File Reputation;
- технология сравнения и анализа поведения;
- Smart Feedback.

Рассмотрим подробнее, как работают эти технологии.

Технология Web Reputation отслеживает надежность сайтов и веб-страниц, используя сведения о репутации доменов, содержащиеся в одной из крупнейших в мире баз данных. Она оценивает репутацию веб-доменов и отдельных страниц, а также ссылок на сайтах (поскольку законные сайты периодически частично взламываются) и блокирует доступ пользователей к сомнительным или зараженным сайтам.

Технология Email Reputation проверяет IP-адреса по базе данных, содержащей сведения об их репутации, и оценивает репутацию отправителей почтовых сообщений в режиме реального времени. Она постоянно анализирует IP-адреса, переоценивая репутацию, и бло-

кирует вредоносные почтовые сообщения и угрозы (например, «зомби») в «облачной» среде до их проникновения в систему.

Технология File Reputation проверяет репутацию всех файлов по «облачной» базе данных, прежде чем предоставить пользователям доступ к ним. Она минимизирует время задержки при проверке благодаря использованию высокопроизводительных сетей для доставки содержимого и локальных серверов кэширования; использует архитектуру «облако — клиент», чтобы уменьшить размер файла локальной антивирусной базы данных и таким образом свести к минимуму угрозу увеличения объемов (большое количество создаваемых за день угроз).

Технология сравнения и анализа поведения сравнивает сочетания действий и компоненты угрозы и определяет, являются ли они вредоносными; постоянно выполняет обновление множества баз данных угроз, обеспечивая реагирование на угрозы в режиме реального времени.

Программа Smart Feedback — это усовершенствованная комплексная защита пользователей, которая обеспечивается благодаря круглосуточному взаимодействию продуктов Trend Micro, исследовательских центров и технологий. Информация обо всех новых угрозах, обнаруженных на клиентских компьютерах в ходе плановых проверок, автоматически заносится в вирусные базы данных Trend Micro.

Данные об угрозах непрерывно собираются посредством глобальной сети, которая включает приманки, средства отправки сообщений, схемы обратной связи, технологии программного просмотра веб-страниц, а также клиентов, партнеров и исследовательских центров TrendLabs.

Специалисты исследовательских центров TrendLabs, а также служб технической поддержки собирают и анализируют данные об угрозах в режиме реального времени посредством запросов в базы данных вредоносных программ компании Trend Micro.

Продукты компании Symantec

Согласно отчету Symantec об угрозах интернет-безопасности, в 2010 году зафиксировано более 286 млн уникальных вредоносных программ. Из-за огромного числа вредоносных программ традиционные решения на основе сигнатур зачастую не справляются с основной задачей. Для обеспечения защиты от новейших угроз Symantec Endpoint Protection 12 использует усовершенствованную технологию Insight. Эта «облачная» технология определения репутации файлов обеспечивает защиту виртуальных сред, основываясь на данных сообщества пользователей продуктов Symantec. Insight распознает и блокирует новейшие угрозы раньше и с большей точностью, чем любой другой аналогичный продукт корпоративной безопасности. Symantec собирает информацию о том, какие исполняемые файлы существуют в мире, когда они были созданы, каким количеством людей используются, откуда появляются и т.д. Это позволяет без анализа содержимого понять категорию файла — опасный он или нет.

Определяя репутацию файлов и исключая проверенные файлы с высокой репутацией при сканировании, Insight позволяет снизить на 70% нагрузку на рабочую станцию. Используемая технология SONAR, основанная на репутационно-поведенческом подходе, позволяет отслеживать работающие приложения на предмет подозрительного поведения и блокировать уязвимости нулевого дня и узконаправленные угрозы в режиме реального времени. Система обнаружения вторжений, Intrusion Prevention System, блокирует атаки на сетевом уровне, до того, как они могут нанести ущерб.

Гибридные технологии защиты с использованием «облачной» репутационной технологии Insight сегодня представлены как в домашних (Norton), так и в корпоративных (Symantec Endpoint Protection 12) продуктах Symantec для защиты рабочих станций, серверов и других устройств, подключенных к сети. В «облаке» Symantec содержатся анонимные данные о распространении более 2,5 млрд файлов более чем на 175 млн компьютерах клиентов, что позволяет обнаруживать новые угрозы, которые невозможно выявить другими способами, и одновременно значительно экономить вычислительные ресурсы локальной системы. Система автоматически присваивает файлам рейтинги безопасности и выполняет сканирование только файлов, подверженных угрозам, снижая затраты ресурсов до 70%. Эта технология позволила Symantec Endpoint Protection 12 обогнать конкурирующие решения по производительности и уровню защиты в тестах Passmark Software и AV-Test.org.

Symantec Endpoint Protection 12 использует «облачные» технологии с использованием функции Symantec Insight, которая автоматически определяет файлы с позитивной репутацией, относящиеся к «списку разрешенных», что повышает точность и эффективность сканирования. Новая технология сканирования Insight также позволяет выполнять большинство процессов во время бездействия компьютеров.

Вторая технология (Shared Insight Cache) позволяет производить сканирование любых файлов всего лишь один раз на инфраструктуру. Таким образом, если на нескольких серверах или рабочих станциях есть одинаковые файлы, то лишь на одной машине файл будет просканирован, а на всех остальных машинах сканирование производиться не будет.

Вместе с тем необходимо признать, что служба репутаций не является панацеей. Ведь вполне возможно, что сетевые настройки будут выведены из строя вредоносным программным обеспечением. Стоит отметить, что только использование комплекса всех технологий (проактивной защиты, баз сигнатур, «облачных» технологий) позволит сегодня чувствовать себя защищенным.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor