УДК 311.2

В.Ф. Безмалый

MVP Consumer Security Microsoft Security, Киев

СЕРВИС РЕПУТАЦИЙ

В статье представлены результаты статистического анализа сетевых атак и уязвимостей, вредоносных программ и вирусов в виде графиков, результаты исследования сервиса репутаций, сделаны выводы и рекомендации.

Ключевые слова: *финансы, вредоносный код, угрозы, уязвимости, сервис репутации, браузер.*

Введение

Не секрет, что сегодня написание вирусов давно стало развитым бизнесом. Это своего рода промышленность. Времена хакеров-одиночек давно в прошлом. Нравится нам или нет, но борьба с вирусами – это борьба с международным преступным сообществом. Основная цель вирусописателей сегодня – деньги!

Уже давно наблюдается разделение труда – один находит уязвимости, 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.

22 сентября 2011, Москва - Специалисты лаборатории G Data Security Labs обнаружили на подпольном форуме распродажу сетей дистанционно управляемых злоумышленниками компьютеров – так называемых ботов, которые в случае активации могут вызвать массивную волну вредоносного кода по всей сети Интернет. Так называемый бот-конструктор AldiBot появился в конце августа по цене всего 10 Евро. Часть вредоносного кода очень напоминает знаменитую сеть ZeuS.

Суть предложения: программа-билдер + бот + обновления + помощь в инсталляции = €10. Более того, несколько дней назад цена достигла €5 Евро.

Для новичков хакерских атак, которые не имеют ни малейшего представления, как работают инструменты для организации атаки, он проводит специальный курс «Молодого бойца». Более того, заботливый автор также использует TeamViewer для того, чтобы сделать своих покупателей еще более уверенными и готовыми к атаке. Это очень напоминает своеобразную службу клиентской поддержки для хакеров.

А теперь ближе к делу: наличие такого дешевого вредоносного кода на рынке (цена AldiBot уже опустилась до 5 Евро), делает организацию DDoS-атаки развлечением и легким способом заработать деньги. Молодые хакеры могут купить программу для создания бот-сети вместе с обновлениями и технической поддержкой на деньги, которые были выделены родителями на карманные расходы.

Таким образом, становится понятным резкий, лавинообразный рост, числа вредоносных программ.

И снова факты.

По данным Лаборатории Касперского (рис. 1):

200 000 000 сетевых атак блокируется ежемесячно;

2 000 уязвимостей в приложениях обнаружено только в 2010 году;

35 000 вредоносных программ появляется ежедневно (рис. 2);

19 000 000 + новых вирусов появилось в 2010 году;

30 000+ новых угроз появляется в день;

ежедневно появляется около 70 000 новых вредоносных программ.

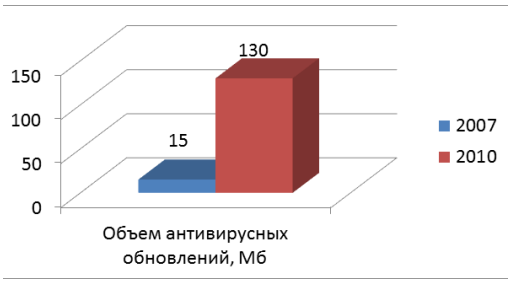

Рис. 1. Объем антивирусных обновлений (по данным "Лаборатории Касперского"

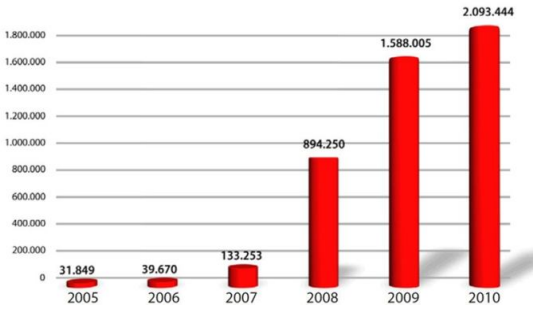

Рис. 2. Рост числа вирусов по версии компании G-Data

Несложно сделать вывод о том, что число вирусов растет лавинообразно. И в данной войне, используя существующие технологии, антивирусные компании скоро придут к тому, что ресурсов ПК будет хватать исключительно на работу антивируса.

Обратимся к истории. С начала 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, что была доля тех, кто заражался раньше, чем получал обновление, но таких было относительно 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 выходит за 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 решить не смогли. **Лучшие примеры реализации эвристического анализа обеспечивают уровень обнаружения в пределах 50-70% для знакомых семейств вирусов и совершенно бессильны перед совершенно новыми видами атак.**

В настоящий момент сформировалось общее видение, что поле борьбы с угрозами, которое сводится к тому, что распознавать угрозы необходимо непосредственно в распределенных центрах обработки данных антивирусной компании, а не только на компьютере конечного пользователя. Такой перенос центра тяжести технологии в Интернет 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, что разработанные технологии существенно сложнее, ведь многие процессы в компьютере требуют времени реакции выше, чем скорость получения подобных обновлений. Кроме этого, необходимо обеспечить защиту в тот момент, когда компьютер вообще не подключен к Сети. Тем не менее, облачные технологии являются ключом к обеспечению безопасности не самых мощных компьютеров, таких как нетбуки, планшеты и смартфоны.

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, так как затраты времени на обнаружение «зловредов», их последующий анализ и тестирование формируемых антивирусных обновлений уже сведены к минимуму.

Что такое сервис репутации?

Сервисы репутации показывают надежность того или иного источника (почта, интернет), показывают репутацию (насколько широко применяется, является ли злонамеренным) того или иного программного обеспечения. При этом вычисление репутации производится на серверах соответствующего производителя в Интернет.

Как это работает?

Рассматривая сервисы репутации, стоит различать облачные сервисы репутации, применяемые сегодня в браузерах Google Chrome, Safari, Opera, Internet Explorer[1] и антивирусные облачные сервисы репутации. И хотя в работе данных сервисов все же есть много общего, однако есть и различия.

Сервисы репутации в браузерах

Рассмотрим, как работают сервисы репутации в различных браузерах.

GoogleChrome

Функция безопасного просмотра Google Chrome, отвечающая за обнаружение фишинга и вредоносного ПО (рис. 3), включена по умолчанию. При попытке посещения сайта, подозреваемого в фишинге или распространении вредоносного ПО, браузер показывает предупреждение.

Рис. 3. Предупреждение о фишинговом сайте в Google Chrome

[1] *В браузере Firefox не реализован облачный сервис репутации, обработка репутации происходит на ПК пользователя (проводится поиск в базах, загружаемых на компьютер пользователя)*

Функция безопасного просмотра защищает вас от фишинга и вредоносного ПО двумя способами. Во-первых, Google загружает в браузер информацию о сайтах, которые могут содержать вредоносное ПО 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 вредоносное ПО 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 запросит 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 бита хэша SHA-256 копии URL). Если компьютер расценит сайт как опасный, будет выдано предупреждение.

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 Google списках опасных сайтов. 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 эту страницу, и URL, совпавший с одним из адресов в списке вредоносного ПО функции Безопасного просмотра Google.

Отключить эту функцию можно в меню «Параметры – Расширенные – Конфиденциальность». Для этого достаточно снять флажок «Включить защиту от фишинга и вредоносного ПО».

Оповещения Google Chrome о фишинге и вредоносном ПО

При включенной защите от фишинга и вредоносного ПО отображаются сообщения, приведенные в табл. 1.

Таблица 1

Сообщения Google Chrome

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

Антифишинговая защита в Opera

В этом браузере для защиты от фишинга используется функция «Защита от мошенничества» (Fraudand Malware Protection), включенная по умолчанию (рис. 4). В начале каждого сеанса с конкретным веб-сайтом она проверяет адрес, используя шифрованный канал (https): передает имя домена и адрес запрашиваемой страницы на специальный сервер, где ищет его в черных списках фишинговых ссылок, формируемых Netcraft (www.netcraft.com) и Phish Tank (www.phishtank.com), а также в списках сайтов с вредоносным ПО, которые ведет «Яндекс».

Если доменное имя совпадет с именем из черного списка, сервер Fraudand Malware Protection возвратит браузеру XML-документ, в котором будет описана проблема (фишинг или вредоносное ПО).

При этом необходимо учесть:

Opera Fraudand 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 «Защита от мошенничества» в меню «Настройки - Расширенные (Crtl-F12) - Безопасность».

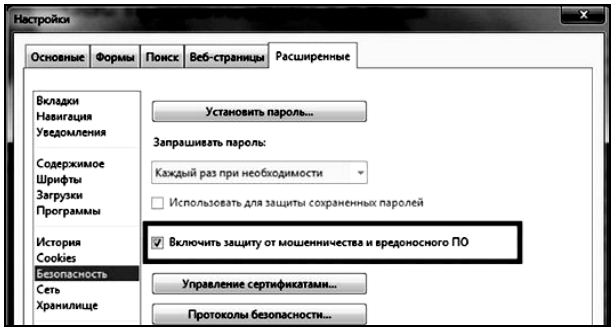

Рис. 4. Антифишинговый фильтр в Opera

Если веб-сайт найден в черном списке, в браузере откроется страница с предупреждением (рис. 5). Пользователю придется решить, посещать эту подозрительную страницу или вернуться на свою домашнюю. Механизм защиты от мошенничества не оказывает никакого воздействия на скорость открытия веб-страниц.

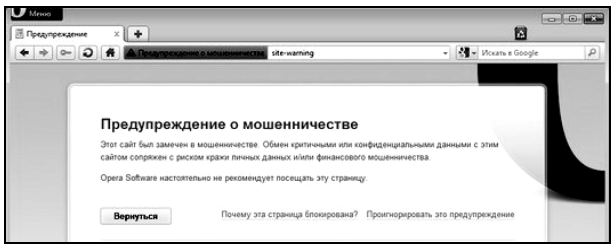

Рис. 5. Предупреждение о мошенничестве в Opera

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 вредоносного ПО. При наличии совпадения пользователь должен увидеть страницу с предупреждением (рис. 6).

Рис. 6. Предупреждение о переходе на сайт, содержащий вредоносное ПО

Фильтр Smart Screen в Internet Explorer 9

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

Фильтр Smart Screen в Interne tExplorer 9 использует сразу несколько технологий. В первую очередь происходит сравнение адреса посещаемого сайта со списком известных мошеннических и вредоносных сайтов. Если сайт найден 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 не подвергаются проверке фильтром SmartScreen.

Для защиты от фишинга и эксплойтов фильтр SmartScreen исследует строку URL целиком, а не подмножество адресов 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 Smart Screen входит и проверка репутации загружаемых файлов Application Reputation Service (ARS).

При загрузке программы в IE9 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, IE9 блокирует закачку, так же, как и IE8. Однако если файл не имеет репутации, IE покажет это в строке уведомления и менеджере загрузки, что позволит принять обоснованное решение о доверии к этому файлу.

Фильтр Smart Screen 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 Smart Screen 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.

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 Smart Screen. В фильтре Smart Screen также 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. Пользователь может решить, следует ли отправлять информацию об узле, который вызывает у него подозрения.

Для защиты от фишинга и эксплойтов фильтр Smart Screen 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 Smart Screen можно включать или отключать избирательно для каждой зоны безопасности, но только в том случае, когда эта функция включена глобально. По умолчанию фильтр Smart Screen включен для всех зон, кроме местной интрасети. Если вы захотите исключить некоторые узлы из списка проверяемых фильтром Smart Screen, 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. Для того чтобы пользователи в организации не могли отключить фильтр Smart Screen, необходимо применить групповую политику.

Сервисы репутаций в антивирусах Kaspersky Security Network

Основные принципы работы 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 по защите от новых угроз.

При помощи KSN автоматически собирается информация о попытках заражения, подозрительных файлах, загруженных и выполняемых на ПК пользователей, независимо от источника их появления (веб-сайты, письма, одноранговые сети и т.д.).

Kaspersky Security Network создана для сбора и передачи информации о попытках заражения. Данная информация передается потом 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 ее 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 (White listing). На схеме (рис. 7) описаны основные принципы взаимодействия KSN с компьютерами пользователей.

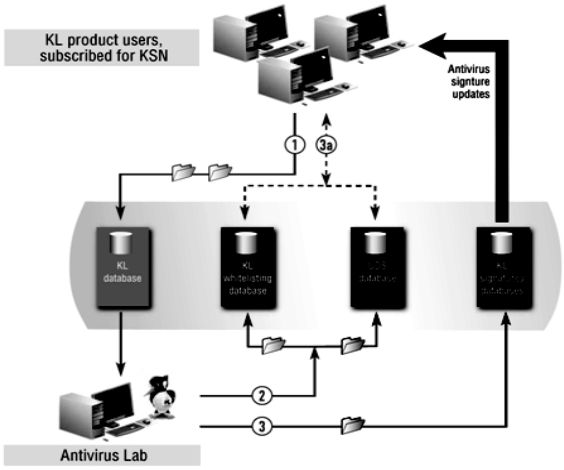

Рис. 7. Схема работы KSN

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 степени 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 широкого 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 сервисов (WoC и GSR).

Trend Micro Smart Protection Network (SPN)

Сервис 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 (рис. 8)

Отслеживает надежность веб-сайтов и веб-страниц, используя сведения о репутации доменов, содержащиеся в одной из крупнейших в мире баз данных.

Оценивает репутацию веб-доменов и отдельных страниц, а также ссылок на веб-сайтах (поскольку законные сайты периодически частично взламываются).

Блокирует доступ пользователей к сомнительным или зараженным сайтам.

Рис. 8. Технология Web Reputation

Технология Email Reputation (рис. 9)

Проверяет IP-адреса по базе данных, содержащей сведения об их репутации.

Оценивает репутацию отправителей почтовых сообщений в режиме реального времени.

Постоянно анализирует IP-адреса, переоценивая репутацию.

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

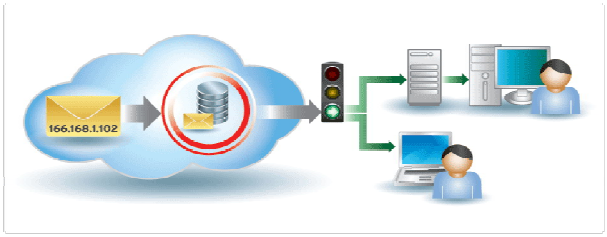

Рис. 9. Технология Email Reputation

Технология File Reputation (рис. 10)

Проверяет репутацию всех файлов по «облачной» базе данных, прежде чем предоставить пользователям доступ к ним.

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).

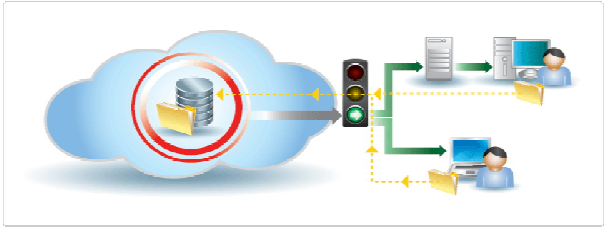

Рис. 10. Технология File Reputation

Технология сравнения и анализа поведения (рис. 11)

Сравнивает сочетания действий и компоненты угрозы и определяет, являются ли они вредоносными.

Постоянно обновляет множество баз данных угроз, обеспечивая реагирование на угрозы в режиме реального времени.

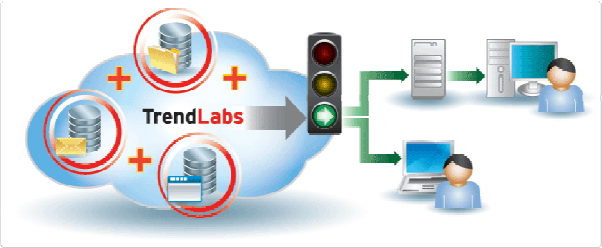

Рис. 11. Технология сравнения и анализа поведения

Программа Smart Feedback (рис. 12)

Улучшенная комплексная защита пользователей 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.

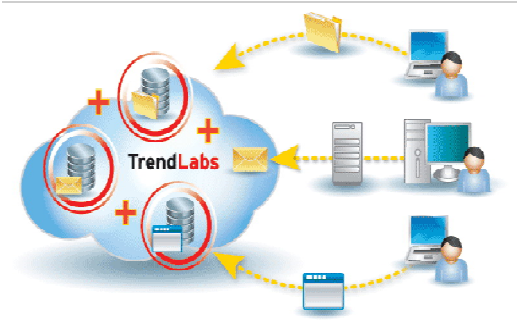

Рис. 12. Программа Smart Feedback

Сбор информации об угрозах

Данные об угрозах непрерывно собираются посредством глобальной сети, которая включает приманки, средства отправки сообщений, схемы обратной связи, технологии программного просмотра вебстраниц, а также клиентов, партнеров и исследовательские центры Trend Labs.

Анализ угроз (рис. 13)

Специалисты исследовательских и сервисных центров Trend Labs, 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.

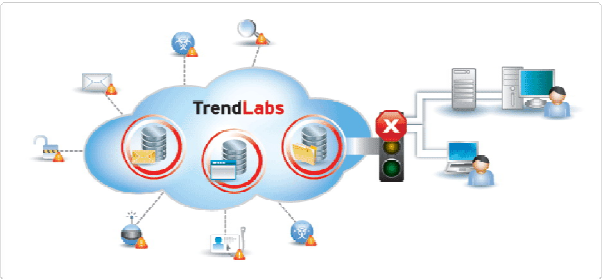

Рис. 13. Анализ угроз

Сервисы репутаций в продуктах компании Symantec

Согласно Отчету Symantec об угрозах Интернет-безопасности, в 2010 году зафиксировано более

286 миллионов уникальных вредоносных программ. Из-за огромного числа вредоносных программ традиционные решения на основе сигнатур довольно часто не справляются с основной задачей.

Для обеспечения защиты от сложных и 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 файл или нет.

Определяя репутацию файлов и исключая проверенные файлы с высокой репутацией при сканировании, Insight позволяет снизить на 70 % нагрузку на рабочую станцию. Также 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 обнаружение 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 миллиардов файлов более чем на 175 миллионах компьютерах клиентов, что позволяет ей обнаруживать новые и неизвестные 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 технологии SymantecInsight, которая автоматически определяет файлы с позитивной репутацией, относящиеся к «разрешенному списку», 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. Т.е. 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.

Вывод

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

Список литературы

1. Безмалый В.Ф. Современные браузеры. Защита от фишинга [Электронный ресурс] / В.Ф. Безмалый // – Мир ПК (Москва). – 2011. – № 7. – Режим доступа к статье: http://www.osp.ru/pcworld/2011/07/13009498/.

2. Безмалый В.Ф. Антифишинговые фильтры в современных браузерах [Электронный ресурс] / В.Ф. Безмалый // Windows IT Pro/RE. – 2010. – № 11 . – Режим доступа к статье: http://www.osp.ru/win2000/2010/11/13006826/.

3. Безмалый В.Ф. Репутации превыше всего! [Электронный ресурс] / В.Ф. Безмалый // Директор информационной службы. – 2012. – № 1. – Режим доступа к статье: http://www.osp.ru/cio/2012/01/13012611/.

Поступила в редколлегию 26.03.2011

Рецензент: канд. техн. наук, доц. С.В. Кавун, Харьковский национальный экономический университет, Харьков.

СЕРВІС РЕПУТАЦІЙ

В.Ф. Безмалий

У статті представлені результати статистичного аналізу мережевих атак і уразливостей, шкідливих програм і вірусів у вигляді графіків, результати дослідження сервісу репутацій, зроблені виводи і рекомендації.

Ключові слова: *фінанси, шкідливий код, погрози, уразливості, сервіс репутації, браузер.*

SERVICE OF REPUTATIONS

V.F. Bezmaliy

The results of statistical analysis of network attacks and уязвимостей are presented in the article, вредоносных programs and viruses as the graphs, results of research of service of reputations, conclusions and recommendations are done.

Keywords: *finances, вредоносный code, threats, to vulnerability, service of reputation, browser.*