Репутации превыше всего!

Владимир Безмалый, независимый эксперт, MVP Consumer Security, Microsoft Security Trusted Advisor; vladb@windowslive.com

Времена хакеров-одиночек давно в прошлом. Сегодня борьба с вирусами превратилась в войну с международным преступным сообществом вирусописателей, и одним из методов в этой борьбе стал сервис репутаций.

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

Сервис репутаций включает следующие технологии.

Whitelisting — белые списки программного обеспечения. С помощью данного решения отслеживаются заведомо безопасные приложения, которые уже проверены антивирусной лабораторией (термин используется «Лабораторией Касперского»). Необходимо подчеркнуть, что белые списки не покрывают всего разнообразия ПО.

Web Reputation — репутация Web-сайтов. Каждой странице присваивается после проверки определенный уровень репутации. Например, сайт часто меняет свой IP-адрес или с него рассылается спам — значит, сайт является подозрительным, соответственно, репутация снижается.

Email Reputation — репутация источника электронной почты. Если с адресов данного домена рассылается вредоносное ПО или спам — репутация домена снижается.

File Reputation — репутация файла. Зависит от источника получения, поведения данного файла и т. д. Если файл получен из сомнительного источника — его репутация заведомо снижена. Если в ходе работы файл пытается несанкционированно записать что-то в реестр либо у разных пользователей файл вроде бы один, но у него разные контрольные суммы — это повод для снижения репутации и т. д.

Smart Feedback — технология сравнения и анализа поведения. Позволяет пополнять базы URL, почтовых адресов и файлов на основе сравнения. Если файлы, загружаемые со страницы, заражены, значит, снижается репутация сайта и наоборот.

На самом деле признаков, по которым вычисляется репутация, намного больше.

КАК ЭТО РАБОТАЕТ?

Предположим, пользователь запускает неизвестный файл. Локальный антивирус проверяет его — файл чист. Однако показывает, что файл странно прописывает себя в реестр, пытается получить доступ к системным сервисам, устанавливает подозрительные соединения.

Сигнал поступает в антивирусное облако, где принимается решение о детекте. В итоге файл блокируется, а его действия откатываются. Или, например, сайт регулярно меняет IP-адрес. В результате все скачанные с его страниц приложения будут иметь сниженную репутацию.

Необходимо отметить, что сервис репутаций сам по себе не является панацеей. Только использование комплекса всех технологий (проактивной защиты, баз сигнатур, облачных технологий) позволит сегодня чувствовать себя защищенным.

ПРИЧИНЫ ПОЯВЛЕНИЯ

Сегодня написание вирусов стало бизнесом и приобрело своего рода промышленные масштабы. Времена хакеров-одиночек давно в прошлом. Нравится нам или нет, но борьба с вирусами превратилась в войну с международным преступным сообществом вирусописателей, чьей основной целью является обогащение.

Здесь даже существует 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…

Число вирусов растет лавинообразно. По данным «Лаборатории Касперского», 200 млн сетевых атак блокируется ежемесячно; 2 тыс уязвимостей в приложениях обнаружено только в 2010 году; более 19 млн новых вирусов появилось в 2010 году; более 30 тыс. новых угроз появляется ежедневно; каждые сутки появляется около 70 тыс. новых вредоносных программ. И в этой войне антивирусные компании, используя существующие технологии, скоро придут к тому, что ресурсов ПК будет хватать исключительно только на работу антивируса.

НЕМНОГО 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, были те, 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, очевидно, что экспоненциальный рост числа новых угроз не оставляет шанса на победу. С одной стороны, объем выпускаемых обновлений выходит за все разумные пределы. С другой стороны, антивирусные компании не в силах наращивать человеческие ресурсы такими же экспоненциальными темпами.

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 проблем решить не смогли. Лучшие примеры реализации эвристического анализа обеспечивают уровень обнаружения в пределах 50–70% для знакомых семейств вирусов и совершенно бессильны перед новыми видами атак.

Сейчас сформировался подход, который 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, разработанные технологии весьма сложны, кроме этого, необходимо обеспечить защиту и в тот момент, когда компьютер вообще не подключен к Сети. Тем не менее облачные технологии являются ключом к обеспечению безопасности не самых мощных устройств, таких как нетбуки, планшеты и смартфоны.

По данным исследования, проведенного во II квартале 2010 года NSS Labs, антивирусным компаниям для блокирования Web-угроз необходимо от 4,6 до 92,5 часа (NSS Labs. Corporate Endpoint Protection Products Group Test: Socially-Engineered Malware Q2 2010, May 17, 2010). В исследовании принимали участие продукты компаний AVG, ESET, F-Secure, «Лаборатория Касперского», McAfee, Norman, Panda, Sophos, Symantec, Trend Micro.

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. CIO.RU