«Автоматическая защита от эксплойтов» для блокирования самых опасных угроз

Одним из наиболее эффективных и опасных способов запуска вредоносного ПО на компьютере жертвы является использование уязвимостей в популярных программах или в самой операционной системе. Такие уязвимости позволяют заразить компьютер в тот момент, когда пользователь выполняет абсолютно, с его точки зрения, безопасную операцию – открывает документ в формате PDF или просто посещает зараженный веб-сайт. При этом наибольшую угрозу представляют так называемые уязвимости «нулевого дня» – прорехи в программном обеспечении, для которых производитель еще не выпустил обновление, решающее проблему.

Для заражения системы посредством уязвимости злоумышленники чаще всего прибегают к массовой рассылке сообщений по электронной почте и в социальных сетях. В таком письме, как правило, содержится ссылка на зараженную веб-страницу или специально подготовленный документ, открытие которого приводит к запуску вредоносного кода. В большинстве случаев злоумышленники используют в качестве «двери» популярное ПО, работающее под ОС Windows – это дает наибольшее количество потенциальных жертв.

Согласно данным «Лаборатории Касперского», две атаки из трех приходятся на программу Adobe Acrobat Reader и виртуальную машину Java, в то время как другое ПО пользуется значительно меньшей популярностью. Такой «выбор» киберпреступников связан с максимальной распространенностью этих программ, причем на различных платформах. В частности, в начале этого года одинаковая уязвимость была обнаружена в версиях платформы Java, работающих как на Windows, так и на компьютерах Apple под управлением Mac OS X. Чуть позже уязвимость привела к эпидемии вируса FlashFake и регистрации первого массового ботнета из зараженных компьютеров Apple.

Значительная часть эксплойтов – вредоносных программ, использующих уязвимости в ПО, может быть заблокирована традиционными средствами антивирусной защиты. Многофункциональное защитное ПО, такое как Kaspersky Internet Security или Kaspersky CRYSTAL, также может блокировать зараженные веб-сайты и фильтровать нежелательную почту с вредоносными ссылками или вложениями. Но для борьбы с самыми сложными вредоносными программами, использующими в том числе уязвимости «нулевого» дня, требуются более продвинутые решения. Именно поэтому в «Лаборатории Касперского» разработали новую технологию «Автоматическая защита от эксплойтов», направленную на борьбу с самыми сложными вредоносными программами – эксплойтами.

О технологии «Автоматическая защита от эксплойтов»

Технология «Автоматическая защита от эксплойтов» предназначена для защиты от вредоносного ПО, использующего уязвимости в программах и операционной системе. В ее основе лежит анализ поведения существующих эксплойтов и сведения о приложениях, которые чаще других подвергаются атакам злоумышленников. За такими программами устанавливается особый контроль - как только одна из них пытается запустить подозрительный программный код, процедура прерывается и начинается проверка.

Запуск исполняемого кода может быть вполне легитимным, например таким образом программа может запросить обновление с сайта разработчика. Чтобы различить обычную деятельность и попытку заражения, новая технология «Лаборатории Касперского» использовала информацию о наиболее типичном поведении известных эксплойтов. Характерное поведение таких вредоносных программ позволяет предотвратить инфекцию, даже если речь идет о неизвестном ранее эксплойте, либо при использовании уязвимости «нулевого дня».

Довольно часто эксплойты перед непосредственным заражением системы осуществляют предварительную загрузку файлов. «Автоматическая защита от эксплойтов» отслеживает обращение к программ к сети, и анализирует источник файлов. Технология может также

различать файлы, созданные при участии пользователя, и новые, неавторизованные. Сответственно, попытка запустить файл, загруженный из подозрительного источника и без ведома пользователя также будет заблокирована.

Еще один используемый в «Автоматической защите от эксплойтов» метод основан на технологии Address Space Layout Randomization (ASLR). Поддержка подобной технологии встроена в операционную систему Windows (начиная с Vista), и обеспечивает случайное расположение ключевых данных (например, системных библиотек) в адресном пространстве, что значительно усложняет использование некоторых уязвимостей. Технология «Лаборатории Касперского» предлагает пользователю функцию Forced Address Space Layout Randomization, которая выполняет те же операции, и способна работать в тех случаях, когда аналогичная система в Windows бессильна. В частности, Forced ASLR может работать и в Windows XP.

Технология «Автоматическая защита от эксплойтов» доступна в новых версиях продукта Kaspersky Internet Security и Антивирус Касперского. Она по умолчанию блокирует запуск любого подозрительного кода, имеющего признаки использования уязвимости в ПО, причем новые методы практически исключают возможность ложного срабатывания. В сочетании с другими инструментами, в частности проверкой веб-страниц и писем на предмет вредоносного кода, «Автоматическая защита от эксплойтов» обеспечивает надежную комплексную защиту от компьютерных угроз, в том числе новых и ранее неизвестных.