ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ЭМУЛЯЦИИ ОТЛАДОЧНЫХ ВОЗМОЖНОСТЕЙ ПРОЦЕССОРА В МОНИТОРАХ ВИРТУАЛЬНЫХ МАШИН

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Козловский М. М.

Шпак И. И. – канд. техн. наук, доцент

Рассматриваются атаки вредоносного программного обеспечения на тестовый стенд, на котором происходит наблюдение за процессом выполнения исследуемых вредоносных программ, или виртуальную среду, организующую его работу, а также уязвимости названных тестовых стендов и виртуальных сред.

Принято считать, что вредоносное программное обеспечение (далее ВПО) включает в свой состав компьютерные вирусы, руткиты, программы-шпионы (Spyware) и вредоносные сетевые приложения [1]. Одной из важнейших задач компьютерной безопасности является борьба с ВПО и, в частности, подзадача его обнаружения. В свете текущих тенденций развития вредоносных программ, все более актуальной становится задача создания эффективного средства обнаружения неизвестного ВПО.

Существующая классификация методик обнаружения ВПО включает поведенческий анализ, который, как правило, реализуется с использованием тестовых стендов, на которых происходит наблюдение за процессом выполнения исследуемых программ. В свою очередь для организации работы тестовых стендов используется виртуальная среда, поскольку по завершению анализа целевой программы данная среда может быть уничтожена без какого-либо риска для аппаратно-программной системы, обеспечивающей ее работу.

С тех пор, как эта методика получила распространение, ВПО стало включать механизмы противодействия, заключающиеся в произведении атаки на тестовый стенд или виртуальную среду, организующую его работу. В связи с этим защита тестовых стендов от подобного противодействия представляет собой актуальную задачу.

Простейшая атака, которую может произвести ВПО на виртуальную среду выполнения программ — обнаружить ее присутствие. Подобное ВПО изменяют логику своего поведения, например, путем отказа от выполнения своих основных функциональных возможностей, что значительно затрудняет его анализ, вводя в заблуждение аналитика.

Большинство виртуальных сред выполнения программ не проектировались с целью быть полностью невидимыми. Они должны быть в достаточной мере прозрачными, чтобы большинство типичного программного обеспечения могло работать под их управлением. Встроенные отладочные возможности процессора не удовлетворяют данным требованиям, поэтому их корректная обработка мониторами виртуальных машин зачастую не требуется.

В качестве примера можно привести механизм отладочных регистров процессоров, построенных по архитектуре IA-32 и AMD-64. При заполнении значений регистров адресами виртуальной памяти возникает аппаратное отладочное прерывание в случае удовлетворения события, связанного с данным виртуальным адресом. Кроме того, допустима установка флага трассировки в регистре флагов, позволяющего отладочному прерыванию возникнуть при выполнении процессором инструкции. Существует также дополнительный флаг записи последнего перехода (Last Branch Record, LBR) в управляющем отладочном регистре. Он позволяет изменить поведение флага трассировки таким образом, что отладочное прерывание возникнет только при выполнении инструкций, производящих изменение регистра указателя текущей инструкции (например, инструкции условных или безусловных переходов, вызова процедуры, возврата из процедуры, явный вызов обработчика прерывания и т.д.). При вызове обработчика отладочного прерывания происходит передача адреса инструкции перехода, вызвавшего прерывание, который впоследствии может обрабатываться операционной системой или ее пользователем.

Многие популярные мониторы виртуальных машин (например, VMware или VirtualBox) некорректно эмулируют данный механизм или не поддерживают эмуляцию отладочных регистров вовсе, как в случае с VirtualBox; отчет о данном дефекте «висит» в системе регистрации ошибок уже в течение пяти лет, и до сих пор не исправлен. Это позволяет обнаружить факт выполнения в виртуальной среде, проверив работоспособность данного механизма. Данная проблема может быть решена путем использования механизмов аппаратной поддержки виртуализации, однако использование этих механизмов открывает другие векторы, позволяющие обнаружить присутствие монитора виртуальных машин [2].

Список использованных источников:

1. Королёв Я.П., Рудский А.В., Масловская А.И. Вредоносное ПО и смартфоны // 49-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 4 мая 2013 года). – Мн.: БГУИР, 2013. – 91 с. с ил. – С. 70-71.

2. Козловский М.М., Шпак И.И. Анализ уязвимостей виртуальных сред выполнения программ // Современные средства связи: материалы XVIII Междунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 322 с. – С. 229-230.