В. С. Матвеева

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ ВСТРОЕННЫХ МЕХАНИЗМОВ РАЗГРАНИЧЕНИЯ ДОСТУПА ОС MICROSOFT WINDOWS

Согласно статистике, опубликованной институтом SANS Institute [1], с момента появления нового способа вторжения в операционную систему (ОС) и до момента выпуска обновления для средства ее предотвращения ОС является уязвимой к атакам нулевого дня в среднем от одного до восьми часов, а иногда этот временной промежуток достигает нескольких месяцев. На сегодняшний день важно, чтобы средство защиты предоставляло в первую очередь проактивную защиту системы, которая в большинстве своем базируется на перехвате системных функций. Данный подход к обеспечению защиты является недокументированным и неуниверсальным, так как многие образцы вредоносного программного обеспечения уже обходят его.

Основной идеей предлагаемого средства защиты является не дать недоверенному процессу в ОС прав и привилегий для выполнения своих функциональных возможностей. В ОС Microsoft Windows реализован сертифицированный механизм разграничения доступа, основанный на маркере доступа со стороны субъекта доступа и списке контроля доступа (далее — ACL) со стороны объекта доступа. При доступе к объекту ОС монитор состояния защиты проверяет, содержится ли уникальный идентификатор пользователя, который является одним из полей маркера доступа, в списке контроля доступа объекта доступа. А далее в соответствии с прописанными в ACL правами доступа для данного пользователя процессу предоставляется или не предоставляется доступ к объекту [2]. Однако большлой минус изложенного механизма в том, что субъектом доступа всегда является пользователь и при загрузке ОС всем процессам присваивается один и тот же уникальный идентификатор пользователя. Поэтому если процесс вредоносной программы запускается в ОС, он имеет те же права и привилегии, что и текущий пользователь. В предлагаемой системе предотвращения вторжений свой уникальный идентификатор генерируется для каждого процесса, и права и привилегии назначаются отдельно для каждого процесса. Это позволяет предоставить процессу доступ только к тем объектам, которые ему необходимы, и назначить ему минимальные привилегии для успешного выполнения. Дополнительно реализована возможность ограничения сетевых взаимодействий каждого процесса с определенными IP-адресами, доменными именами, по определенным портам и т. д. Таким образом, каждый процесс функционирует в своем собственном контексте защиты, и это предотвращает успешное выполнение вредоносного кода, основанное, как правило, на внедрении кода в другие процессы, перехвате функций, загрузке драйверов, загрузке файлов с вредоносных интернет-ресурсов и так далее, что не выполняется по причине недостаточных привилегий. При этом стоит отметить, что разработанная система потребляет минимальное количество системных ресурсов по сравнению с другими средствами защиты, но предъявляет высокие требования к компетентности пользователя, который осуществляет ее настройку.

Предлагаемая система может эффективно использоваться в предотвращении очень распространенного на сегодняшний день вида мошенничеств, связанных с системами ДБО и основанных на удаленном управлении и/или несанкционированном копировании данных, необходимых для аутентификации в них. Рабочая станция бухгалтера настраивается один раз для основных процессов, используемых им в работе, и создание любого нового процесса предотвращается или его выполнение ограничивается по максимуму.

В результате модификации встроенного в ОС механизма разграничения доступа строится универсальный способ предотвращения вторжений, который работает в том числе и для атак нулевого дня.

СПИСОК ЛИТЕРАТУРЫ:

1. *Hofman M.* Survival time: международные публикации института SANS. SANS Institute. 2009. URL: http://isc.sans.edu/survivaltime.html.
2. *Russinovich M., Solomon D.* Windows Internals: Covering Windows Server 2008 and Windows Vista. 5th edition. Microsoft Press. 2009. P. 420–491.

М. Р. Мухтаров

ПРИМЕНЕНИЕ ИММУННОГО ПОДХОДА В ЗАДАЧЕ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ

В работе предложен подход применения алгоритма негативной селекции для выявления аномалий в данных о сетевом трафике, полученных средствами протокола IPFIX. Для решения данной задачи предлагается способ формализации алгоритма генерации детекторов согласно формату экспорта данных о сетевом трафике протокола IPFIX.

Объектом исследования является типовая архитектура инфраструктуры «облачных вычислений» на базе средств с открытым исходным кодом: операционные системы на базе ядра операционной системы Linux, протокол доступа к хранилищам данных по сети Интернет, свободно распространяемые средства виртуализации. Основные угрозы информационной безопасности инфраструктуры «облачных вычислений» связаны с проблемой использования разделяемых аппаратных, программных и сетевых ресурсов [1]. Таким образом, существует необходимость поиска подхода к мониторингу событий информационной безопасности внутри инфраструктуры «облачных вычислений». В работе [1] был предложен подход размещения датчиков IPFIX в составе инфраструктуры «облачных вычислений», который подразумевает использование датчиков на «виртуальных сетевых интерфейсах».

Алгоритм профилирования сетевого трафика в рамках инфраструктуры «облачных вычислений» на основе данных, полученных средствами протокола IPFIX, предложен в работе [2]. В основе алгоритма лежит метод максимизации энтропии, описанный в работе [3]. В докладе предлагается решение задачи регистрации аномалии с использованием алгоритма негативной селекции, впервые описанной в работе [4]. Алгоритм негативной селекции является одним из подходов применения искусственных иммунных систем и основан на принципе уничтожения детекторов соответствующих нормальному профилю и сохранению детекторов, отличающихся от него [4]. Применение искусственных иммунных систем в задачах обнаружения вторжений и сетевых атак было предпринято в ряде работ [5–9]. В данной работе делается попытка комбинированного подхода, построения нормального профиля с использованием метода максимизации энтропии и алгоритма негативной селекции. В дополнение развивается подход размещения датчиков IPFIX на интерфейсах виртуальных машин, что актуально для решения задач регистрации аномалии в инфраструктуре «облачных вычислений».

СПИСОК ЛИТЕРАТУРЫ:

1. *Mukhtarov M., Miloslavskaya N., Tolstoy A.* Network security threats and Cloud Infrastructure Services Monitoring // IARA 2011. 22 May 2011. P. 141–145.