Н. П. Васильев, Д. С. Сильнов

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ СИСТЕМ УДАЛЕННОГО МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ

Введение

Системы мониторинга любого объекта выполняют множество задач, в том числе и контроль работоспособности наблюдаемого объекта. В случае нарушений в системе мониторинга невозможно отследить возникающие проблемы, которые в большей или меньшей степени вызывают потери различного рода (финансовые, потери данных и другие), в особенности в системах ответственного назначения. Работоспособность систем мониторинга может быть нарушена из-за ряда ситуаций, значительную часть из которых возможно обнаружить и устранить с помощью программных средств.

С развитием систем контроля поведения (антивирусы, межсетевые экраны и другие) появилась опасность нарушения функционирования систем мониторинга при их совместной работе. Одной из причин этого являются частые ложные срабатывания антивирусов и межсетевых экранов [1]. Даже при качественной настройке систем контроля поведения ложные срабатывания, к сожалению, имеют место. Это увеличивает вероятность того, что обычное программное обеспечение (в том числе и системы мониторинга), которое не имеет собственной дополнительной защиты, может быть ограничено в доступе к ресурсам или его работа аварийно завершена. В ответственных системах, где необходимо производить бесперебойный мониторинг, это недопустимо.

Отключение систем контроля поведения не представляется возможным, так как они защищают систему от вредоносного ПО и различного рода атак. Поэтому необходимо обеспечить совместное функционирование этих двух видов систем, но при этом оградить системы мониторинга от воздействия со стороны систем контроля поведения. Это возможно в том случае, если система мониторинга работает через каналы, которые не отслеживаются системами контроля; в противном случае гарантий стабильной работы практически нет. Для этого используются программные средства защиты, которые и обеспечивают работу систем мониторинга вне зависимости от внешних условий.

Рассмотрим существующие области конфликта систем контроля и систем мониторинга, а также существующие средства защиты в этих областях и насколько они решают поставленные задачи. Такими областями являются:

- связь между клиентом и сервером;
- доступ к ресурсам ЭВМ.

Связь между клиентом и сервером осуществляется без помех в случае отсутствия специальных средств контроля поведения и ограничена лишь периодичностью доступа клиента и сервера к сети Интернет. В случае наличия средств контроля поведения, когда не происходит умышленного блокирования системы мониторинга, системами защиты используются недостатки настроек систем контроля поведения. Взаимодействие осуществляется либо напрямую, либо с использованием сторонних процессов (например, iexplore.exe) для передачи данных от их имени. Подобную технику часто применяют вредоносные программы (вирусы, троянские программы) [2]. В случае, когда идет умышленное блокирование системы мониторинга либо же полное блокирование всех процессов для работы с сетевыми функциями, нет возможности сохранить работоспособность системы мониторинга. Таким образом, современные средства защиты не могут обеспечить работоспособность систем удаленного мониторинга в случаях умышленного блокирования или отсутствия недостатков в настройке систем контроля.

Доступ клиента к ресурсам ЭВМ может быть также ограничен системами контроля поведения. Это может быть, например, приостановка работы процесса или частичная блокировка

ресурсов. Современные системы защиты могут противостоять остановке работы, но не позволяют бороться с блокированием доступа к ресурсам, как в случае умышленного ограничения. Многие антивирусы (например, Kaspersky Antivirus [3]) могут запретить доступ к файлам так, что средства защиты не смогут обеспечить доступ, и работоспособность приложения нарушится.

Построим ER-модель [4] классификации существующих методов защиты систем удаленного мониторинга. Методы защиты следует классифицировать по двум основным направлениям — по защищаемой области и по расположению элементов защиты (Рис. 1).

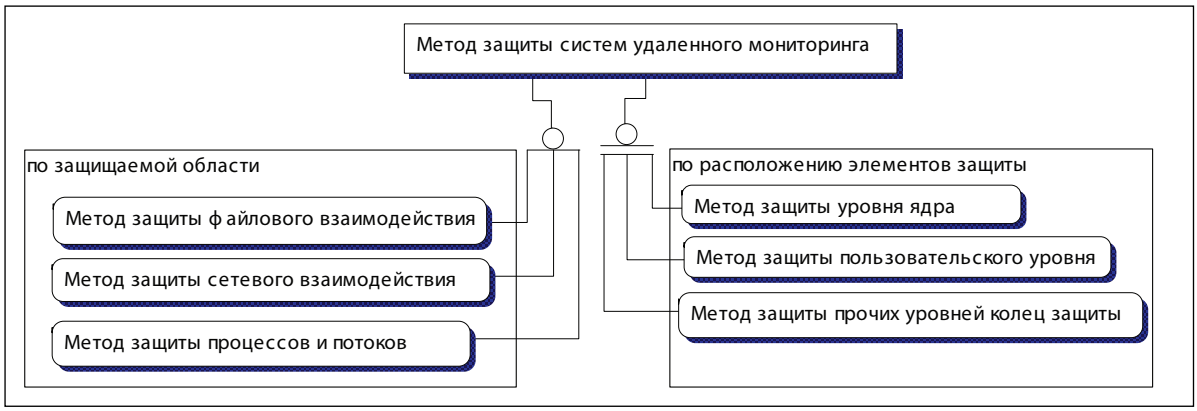

Рис. 1. ER-диаграмма классификации методов защиты

Рассмотрим более подробно каждый из элементов данной классификации.

Методы защиты файлового взаимодействия. Один из таких методов заключается в обходе систем контроля за счет внедрения в чужой процесс. Например, распространенным способом реализации данного метода в ОС семейства Windows является внедрение в процесс svchost.exe, которому разрешена любая активность. Данная процедура позволяет обеспечивать взаимодействие с файловой подсистемой, используя недоработки в системах контроля поведения. Другой же метод состоит в том, что необходимо обозначить точки, в которых осуществляется воздействие со стороны систем контроля, и по возможности обеспечить взаимодействие с файловой подсистемой в обход данных точек.

Методы защиты сетевого взаимодействия. Из существующих методов один был уже упомянут выше — это внедрение в чужие процессы с целью исполнения в контексте процесса необходимых действий. Это делается для того, чтобы обойти запрещающие правила систем контроля поведения. Чаще всего это процессы, которым системами контроля поведения по умолчанию разрешен доступ в Интернет, например, браузеры (iexplore.exe, firefox.exe и др.), почтовые клиенты (thebat.exe и т.п.). Второй метод (в случае функционирования элемента системы защиты в виде драйвера) позволяет использовать API (интерфейс прикладного программирования) режима ядра для создания соединений и сетевого взаимодействия; подобный подход используется, к примеру, в вирусе Rustock. В том случае, когда системы контроля не имеют «врезок» на уровне NDIS (драйвер сетевой подсистемы в ОС семейства Windows), а используется замена адресов функций в GDT (глобальная таблица дескрипторов), этот метод успешно работает, так как замена в GDT будет эффективна только для приложений пользовательского уровня.

Методы защиты процессов и потоков. Методов существует несколько, один из них заключается во внедрении в чужие потоки либо в создании потока в рамках другого процесса. Кроме этого, существует подход, когда создается процесс без окна, он по-особому отображается в диспетчере задач. В то же время, для систем контроля поведения он является обычным процессом, как следствие, данный подход не дает значимых преимуществ.

Методы защиты пользовательского уровня. На данном уровне не так много методов защиты, потому что здесь нет возможности влиять на системные параметры ОС. Таким образом, системы контроля, которые располагаются на уровне ядра, имеют значительно больше возможностей, и на пользовательском уровне нет гарантированных методов успешной защиты от них.

Методы защиты уровня ядра. Существующих методов не так много из-за сложности реализации, а также большого объема знаний, требуемых для создания драйверов на уровне ядра. Одним из существующих методов является метод обращения и взаимодействия через TDI (транспортный интерфейс для драйверов).

Методы защиты прочих уровней. Занимая промежуточное положение, прочие уровни колец защиты не имеют функционала, который есть на уровне ядра, но имеют определенные ограничения. Кроме этого, из режима уровня ядра возможно полное управление ПО, функционирующим на прочих уровнях, что не является положительным моментом данного подхода.

Заключение

Проблема плохой настройки систем контроля поведения будет существовать всегда из-за того, что нельзя сформировать идеальные правила для любых условий. Хотя разработчики антивирусных продуктов пытаются решить данную проблему за счет обучаемых адаптивных систем, динамически подстраивающихся под каждую систему в отдельности, этот метод лишь уменьшает число плохо настроенных систем, а не решает проблему полностью. Таким образом, существующие средства защиты систем удаленного мониторинга в ряде случаев решают поставленные перед ними задачи, но основная масса проблем может быть решена только за счет разработки новых средств.

Одним из наиболее перспективных решений существующих проблем является организация передачи данных (по сети и к файловой системе) в обход систем контроля поведения. Это позволит не зависеть от межсетевых экранов и антивирусов и обеспечит беспрепятственную работу для систем удаленного мониторинга. Подобное решение может быть достигнуто путем поиска и анализа точек контроля, в которых системы контроля поведения производят перехват запросов и построение модели взаимодействия в обход данных областей.

СПИСОК ЛИТЕРАТУРЫ:

1. PCSL Greater China Region False Positive Test. URL: http://www.pcsecuritylabs.net/document/report/2011_JAN_Greater_China_Region_False_Positive_Test_English.pdf.
2. «Лаборатория Касперского» сообщает об обнаружении нового буткита. URL: http://www.cybersecurity.ru/crypto/119305.html.
3. www.kaspersky.ru.
4. *Blaha M.* Patterns of Data Modeling (Emerging Directions in Database Systems and Applications). CRC Press, 2010.