Защита программ на основе гипервизора

Небогатиков И. Ю., студент кафедры системного программирования СПбГУ, ivan.nebogatikov@gmail.com

Под руководством Ханова А. Р.

Аннотация

Вредоносное программное обеспечение, использующее уязвимости в защитах операционных систем, представляет особую опасность, поскольку может модифицировать защитные средства. В данной работе представлено средство защиты на основе гипервизора от подмножества таких вирусов, модифицирующих таблицу системных прерываний, читающих защищенные файлы и пытающихся выгрузить системы защиты.

Введение

Современные операционные системы Linux и Windows используют 2 кольца доступа для разграничения прав доступа: Кольцо 0, для работы ядра системы, и Кольцо 3, для пользовательских программ. В ядро системы часто добавляются новые модули, различные драйверы. Этот подход позволяет злоумышленникам повысить свой уровень привилегий получить доступ к системным ресурсам и другим программам. Такое программное обеспечение называется руткитом.

Использование для защиты ПО с тем же уровнем привилегий не эффективно, поскольку руткит может модифицировать его. Для решения задачи можно воспользоваться технологиями виртуализации и создать еще одно, -1 Кольцо защиты. Такой подход не позволяет руткиту изменять защитное ПО.

Эти методы широко используются для защиты программ, работающих в режиме ядра. Например, фреймворк Shadow-Box [1] для защиты ядра Linux, после проверки безопасности при загрузки, позволяет маскировать физические страницы процессов и проверять модификацию регистров GDTR, LDTR, IDTR и MSR.

HyperForce [2] использует для защиты исполняемого кода следующий подход: защищаемый для исполнения код загружается в виде отдельного модуля ядра Linux, с помощью VMM создается виртуальное

устройство, а обращения к критическому коду заменяются на прерывания этого устройства.

Описание векторов атаки

- Системные вызовы

  Один из способов нарушение функциональности операционной системы — перехват системных вызовов. Он осуществляется с помощью поиска и подмены таблицы системных вызовов. Информацию о ее расположении можно получить из MSR (Machine State Register) регистров MSR_LSTAR и MSR_CSTAR в которых хранится адрес обработчика прерываний для процессоров архитектуры x86-64.

  Для операционной системы Linux подробнее описано в [3].

  Руткит VirtualDbgHide [4] эксплуатирует этот вектор атаки и меняет ссылку на таблицу системных вызовов в операционной системе Windows 8.1, оставаясь незамеченным для системы защиты PatchGuard.

- Модификация файлов

  Повысив свой уровень привилегий, руткит может модифицировать файлы, даже если они защищены ограничением прав доступа.

- Отключение системы защиты

  Для ОС система защиты выглядит как набор сервисов, поэтому каждый пользователь, обладающий правами администратора, может отключить все элементы зашиты.

Гипервизор HyperPlatform

Для защиты используется гипервизор с открытым исходным кодом HyperPlatform [5], разрабатываемый для исследований операционной системы Windows. Он позволяет отслеживать события обращения к памяти, регистрам, выполнения некоторых процессорных инструкций, прерывания.

Гипервизор используется для:

1. анализа руткитов;

2. реверс-инжиниринга ядра ОС;

3. разработка системы предотвращения вторжений (VIPS).

Реализация

Система защиты предназначена для работы с антивирусом КОДА, который состоит из двух частей, работающих в пользовательском и привилегированном режимах ОС Windows. Его основная задача — фильтрация вредоносного поведения программ. Не смотря на это, он не защищен от уязвимостей, описанных выше.

Тем не менее, система может быть использована для защиты любого ПО, работающего в режиме ядра.

Основная защита

При системных вызовах вызывается обработка инструкции VMExit [6] гипервизора, при этом известна причина вызова обработичка. Поэтому можно отфильтровать все запросы и выделить среди них те, которые читают или пишут в регистры MSR_LSTAR и MSR_CSTAR.

При попытке записи в эти регистры, создается локальная скрытая копия изначальных значений, которая будет возвращаться при последующих попытках чтения.

Поскольку система защиты может использоваться для работы с ПО, в задачи которого может входить модификация этих MSR регистров, надо оставить возможность изменять их. Чтобы определить, какая именно программа записывает новые значения используется проверка регистров общего назначения. В гипервизоре и приложении до компиляции записывается информация об используемых регистрах и их значениях. При полном совпадении программе разрешается внести изменения в регистры MSR_LSTAR и MSR_CSTAR.

Драйверы-фильтры

Для защиты файлов приложения был создан драйвер-фильтр [7] файловой системы. При его компиляции необходимо указать список папок, доступ к которым должен быть ограничен. При обращении к файлам происходит проверка, находится ли исполняемый файл внутри одной из данных папок, и в данном случае ему предоставляется доступ.

Надо ограничить возможность пользователя так, чтобы только защищаемое приложение знало о наличии защиты. Созданные драйвера не должны быть видны в общем списке сервисов. Для этого был создан драйвер-фильтр, который скрывает наличие в системе себя и двух вышеописанных драйверов.

Отключение всех драйверов возможно через защищаемое приложение, для этого проверяются имя программы и путь ее исполняемого файла.

Заключение

В работе было представлено средство защиты на основе гипервизора от руткитов для операционной системы Windows.

Текущие результаты представлены в GitHub-репозитории [8].

Литература

[1] Kelly S., Tolvanen J.-P. Myth and Truth about Hypervisor-Based Kernel Protector: The Reason Why You Need Shadow-Box. — Black Hat Asia 2017 — URL: https://www.blackhat.com/docs/asia-17/materials/asia-17-Han-Myth-And-Truth-about-Hypervisor-Based-Kernel-Protector-The-Reason-Why-You-Need-Shadowbox-wp.pdf (дата обращения: 01.04.2019г).

[2] KFrancesco Gadaleta, Nick Nikiforakis, Jan Mühlberg, Wouter Joosen. HyperForce: HypervisorenForced Execution of Security-Critical Code. Dimitris Gritzalis; Steven Furnell; Marianthi Theoharidou. 27th Information Security and Privacy Conference (SEC), Jun 2012, Heraklion, Crete, Greece. Springer, IFIP Advances in Information and Communication Technology, AICT-376, pp.126-137, 2012, Information Security and Privacy Research. — URL: https://hal.inria.fr/hal-01518236/document (дата обращения: 01.04.2019г).

[3] Перехват системных вызовов в linux под x86-64. — URL: https://habr.com/ru/post/110369/ (дата обращения: 01.04.2019г).

[4] Репозиторий VirtualDbgHide. — URL: https://github.com/Nukem9/VirtualDbgHide (дата обращения: 01.04.2019г).

[5] Репозиторий HyperPlatform. — URL: https://github.com/tandasat/HyperPlatform (дата обращения: 01.04.2019г).

[6] Intel 64 and IA-32 Architectures Developer's Manual: Combined Vols. 1, 2, and 3. Intel, 2018.

[7] Документация Windows Driver Model. — URL: https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/windows-driver-model (дата обращения: 01.04.2019).

[8] GitHub-репозиторий. — URL: https://github.com/Ivan-Nebogatikov/HyperPlatform (дата обращения: 01.04.2019).