электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 003.26.7 004.9

Защита встроенных систем на основе подхода «Симбионт»

Кондратюк П. А., *студент,*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Попко К. С., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Алешин В. А., к. т. н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
v.a.matveev@bmstu.ru

Практически все современные IP телефоны фирмы Cisco, включая те, которые используются в США в правительственных кругах и Белом доме, имеют уязвимости, которые позволяют злоумышленникам получить полный контроль над устройством. Ученые из Колумбийского университета разработали средство, которые они назвали симбиотическим - “symbiote” (далее по тексту: Симбионт) и, которое позволяет определить атаку [4].

Недавнее исследование показало, что существует огромное количество незащищенных аппаратных средств в Интернете, в первую очередь это маршрутизаторы, которые при небольшом желании можно легко взломать. Несколько новых уязвимостей в Cisco IOS продемонстрировали незащищенность огромного количества маршрутизаторов высокого класса защищенности. В [1] предлагается новый метод для обнаружения и защиты от новых угроз инфраструктуры маршрутизации в Интернете, а также для огромного количества других сетевых устройств.

Симбионт является экспертной системой для обнаружения вторжений в прошивку системы. Оно также чувствительно к несанкционированным модификациям прошивки устройства. Внедрение кода Symbiote осуществляется в исходный код с помощью случайного распределения так, чтобы каждый экземпляр отличался ото всех других внедренных систем для того, чтобы предотвратить попытки злоумышленника отключить его. Симбионт, начиная с момента активации внутри программного оборудования или

хостовой программы, обеспечивает следующие четыре фундаментальных свойства безопасности:

1. Имеет полностью прозрачный код и режим работы хостового приложения, и может как пассивно контролировать, так и активно реагировать на происходящие события в системе.

2. Работает одновременно с программным оборудованием или хост-программой.

3. Код Symbiote не может быть изменен или отключен посторонними лицами через онлайн или оффлайн атаки.

4. Каждый раз, когда Symbiote создается, его код распределен случайным образом в системе и приспособлен к текущим условиям.

В качестве модели угроз используется следующая.

Предполагается, что злоумышленник технически искусен и ознакомлен с имеющимися уязвимостями (в том числе «нулевого дня»), а также с совместимыми эксплойтами, реализующими гарантированное выполнение произвольного кода. Также предполагается, что атаки осуществляются в онлайн режиме.

Другими словами, злоумышленник должен провести удаленную атаку на рабочее устройство, не вмешиваясь в его функции или вызывая его сбой или перезагрузку. Атаки, включающие в себя изменение конфигурации или полную замену образа операционной системы (что требует перезагрузки) из модели исключены, так как они могут быть обнаружены обычными способами. Также допущено, что злоумышленник имеет доступ к исходному образу программной среды, еще до того, как Симбионт был в нее внедрен.

Онлайн атаки на защищаемый хост могут быть разделены на две категории: те, что пытаются отключить или обойти Симбионт, защищающие хост, и атаки, которые этого не делают.

Что касается маршрутизаторов Cisco, атаки происходят с помощью руткитов, которые вносят изменения в операционную систему IOS. Симбионт может использоваться для обнаружения внедренного кода, который изменяет статические части устройства. В этом случае Симбионт предназначен только для обнаружения несанкционированной модификации кода. Однако он также может быть использован для обнаружения внесенных изменений и в динамические области: стек и кучу.

Принцип работы Симбионта следующий.

Симбионту периодически предоставляется ЦП для выполнения. После того, как вызван Симбионт-менеджер, он выполняет небольшую часть задачи по защите а затем

возвращает управление обратно прерванной хост-программе. Это позволяет Симбионту и хост-программе выполняться одновременно, причем он не влияет на функциональность основной хост-программы. Симбионт, находящийся в той же среде выполнения что и хост- программа, имеет возможность пассивно контролировать или вносить изменение в поведение хост-программы во время выполнения. Как только Симбионт встроен в защищаемую хост-программу, попытки испортить или изменить двоичный код Симбионт будут либо обнаружены им, либо произойдет аварийное завершение хост-программы.

Симбионт может защитить любой произвольный исполняемый код, в том числе и другие экземпляры. В отличие от традиционных антивирусных и хост-защитных механизмов, которые устанавливаются и в значительной мере зависят от средств, предоставляемых системами, он рассматривает свою хост-программу как внешнюю и ненадежную сущность. Симбионт не зависит от функциональности хост-программы, и это дает ему несколько важных следующих преимуществ.

1. *Независимость от операционной среды*. Поскольку Симбионт внедряется в свою хост-программу, его не нужно приводить к любому исполняемому формату. Симбионт будет запускаться , если будет запускаться его хост-программа, независимо от типа операционной системы и ее версии.

2. *Может находиться в пределах любого исполняемого кода, независимо от его функциональности или положения в стеке системы*. Уникальный механизм встраивания позволяет тому же Симбионту действовать в рамках пользовательских приложений, драйверов устройств, ядра и даже других Симбионтов . Кроме того, могут функционировать сразу несколько Симбионтов на разных уровнях, что открывает новый подход развертывания защиты в глубину.

3. Может быть легко и безопасно внедрен в операционные системы, рассматриваемые как «Черный ящик».

4. *Самодостаточен, и не зависит от средств, предоставляемых его хост-программой.* Симбионте не использует какой-либо внешний код для защиты своего хоста, и следовательно, неуязвим для атак на другие части системы .

5. *Обладает самозащитой и скрытностью,* его трудно обнаружить и деактивировать злоумышленнику.

6. *Эффективность работы*. Использует вычислительный ресурс устройства напрямую, не через ОС, или виртуальную машину, на которой запущена ОС.

Симбионт состоит из следующих частей: перехватчика контроля потока, менеджера и кода. Все вместе, они изначально загружаются в защищаемое устройство.

Процесс внедрения может быть проведен в оффлайн-режиме (создает новую защищенную прошивку) или динамически (во время использования системы, как часть командной оболочки). На практике, внедрение может быть произведено с минимальными изменениями системы. Поскольку Симбионт встраивается в систему изначально, размер полученной прошивки не изменяется. В качестве примера можно привести последнюю версию Симбионта - Doppelganger, которая наряду со средством обнаружения руткитов, занимает лишь 1384 байт.

В целом, Симбионт не зависит от особенностей реализации прошивки.

Перехват управления и предоставление ЦП для работы Симбионт осуществляется следующим образом.

Перехват управления осуществляется с помощью внедрения компоненты перехватчик контроля потока. Точки входа перехватчиков контроля потока выбираются случайно в областях реального кода внутри программы главного процессора. От числа перехватчиков зависит частота захвата Симбионтом процессора, а производительность работы всего Симбионта зависит от того, какие части кода определены как реакльные.

Целесообразно обеспечить распределить точки перехвата в областях кода, который будет часто выполняться при работе программы, что, в общем случае, сложно сделать с высокой точностью.

Существуют как статические, так и динамические методы встраивания в исполнительный код. Динамический подход не позволяет определить области кода, которые доступны для встраивания. По этой причине, для определения мест внедрения, выполняется статические методы контроля потоков главной программы.

Основные методы внедрения Симбионта следующие. Симбионт внедряется в большое число случайных частей для того, чтобы периодически предоставлять ЦП для обнаружения вредоносного кода. Такой подход позволяет Симбионту оставаться незамеченным операционной системе во время обработки загруженных им данных. Оно имеет полный доступ к внутренним данным ОС, но не только, что позволяет эффективно выполнять код, что недостижимо при работе в ОС. В силу этого, средство обнаружения руткитов для IOS может обходит ограничения системы безопасности, т.к. это средство работает извне ОС.

Такие уловки являются мощной частью структуры Симбионта. В случае IOS, ни одно средство диагностики, доступное в ОС, неспособно определить присутствие кода СВС, т.к. он не затрагивает специфических структур системы и невидим для ОС. В дальнейшем, процессы, запущенные Симбионт, скрываются, поскольку уведомлений об

обработке вредоносного кода главным процессором не предусматривается в ОС и поскольку код распределен случайным образом в большом количестве несвязанных между собой процессов.

С помощью использования расширения Симбионта — Doppelganger, можно автоматически внедрить средство обнаружения руткитов в маршрутизатор Cisco 7120 при использовании двух основных версий IOS — 12.2 и 12.3. Посредством внедрения 1400 байт кода в прошивку. Doppelganger защищает маршрутизатор от всех попыток подключения (функций), внешних вмешательств и попыток изменения кода. Поскольку Симбионт функционирует совместно с исходной операционной системой устройства, а не внутри неё, оно позволяет внедрить базовые защитные средства вне зависимости от прошивки или программного обеспечения устройства. В силу уникальности сетевых программно-аппаратных средств Cbsco, их распространение с установленным Симбионт ослабит угрозу всемирной системе связи.

Список литературы

1. Ang C., Stolfo S.J. Defending Embedded Systems with Software Symbiotes. Available at: http://ids.cs.columbia.edu/sites/default/files/paper_2.pdf, accessed 27.12.14.
2. Chang, H., Atallah, M. J. Protecting software code by guards. Available at: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2001-49.pdf, accessed 27.12.14.
3. Ang C., Stolfo S.J. Symbiotes and Defensive Mutualism: Moving Target Defense. Available at: http://ids.cs.columbia.edu/sites/default/files/Symbiote-Moving-Target-Defense_2011_2.pdf, accessed 27.12.14.
4. Choi C. Q. Embedded Anti-Malware Defends Against Cisco IP Phone Hack. Available at: http://spectrum.ieee.org/telecom/security/embedded-antimalware-defends-against-cisco-ip-phone-hack, accessed 27.12.14.
5. Janus M. Heads of the Hydra. Malware for Network Devices. Available at: http://securelist.com/analysis/36396/heads-of-the-hydra-malware-for-network-devices/, accessed 27.12.14.