УДК 004.056

Марченко В. А., к.т.н.

ОСОБЕННОСТИ ПРОВЕДЕНИЯ УДАЛЕННЫХ АТАК ТИПА MITB НА РАСПРЕДЕЛЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Институт кибернетики им. В.М. Глушкова НАН Украины

Рассмотрены вопросы, связанные с особенностью проведения информационных атак нового класса MITB на распределенные информационные системы. Описано общая схема проведения атаки данного класса, приведены различия между пассивной и активной атакой в завершающей фазе.

Современные тенденции

В последнее время в области информационной безопасности подавляющее количество происшествий связаны с атаками на различные распределенные информационные системы.

При этом существенное количество успешных атак составляют атаки, проведенные с помощью давно известных атак типа MITM (человек-по-середине), а так же новых классов атак типа MTIB (человек-в-броузере) и в более общем виде MITC (человек-в-клиенте) [1].

Подобные тенденции в области проводимых информационных атак требуют проведения дополнительных исследований связанных с изменением характера реализуемых атак и усложнения их сценариев [2].

Целью статьи является исследование типовых сценариев проведения современных информационных атак. Особенное внимание уделяется анализу реализуемых схем атаки, которые используются для компрометации распределенных информационных систем.

Классы современных информационных атак

Классическая схема проведения MITM-атаки состоит из нескольких этапов. Для реализации описываемой атаки необходимо наличие «клиента» – отправляющего данные, «сервера» – принимающего и обрабатывающего данные, а также вычислительного устройства злоумышленника, которое имеет доступ к используемой среде передачи данных (рис.1). На первом этапе злоумышленник разрывается логический канал связи между отправителем и получателем при этом физические каналы связи могут быть неизменными. Главным условием успешности проведения атаки является отсутствие иных каналов связи между отправителем и получателем, которые могут быть задействованы при проведении сетевого взаимодействия, что может нарушить сценарий проведения компрометации информационного обмена. На следующем этапе проводится перенаправление информационных потоков от получателя и отправителя на систему злоумышленника. При этом следует учитывать, что указанная система должна полностью поддерживать используемый коммуникационный протокол кроме этого, она должна уметь корректно представляется для отправителя корректным получателем, и наоборот, для получателя корректным отправителем [2].

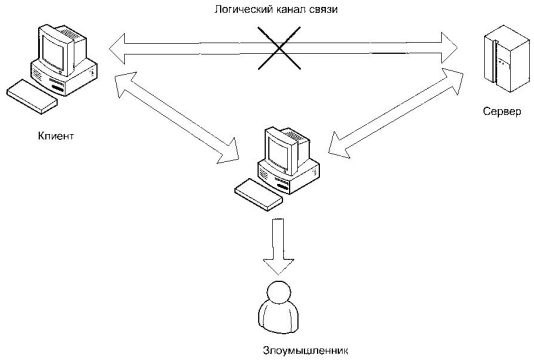

Рис.1. Схема проведения MITM атаки

Данный класс атак считается хорошо изученным и соответственно существует много известных методов и средств для противодействия проведению подобных атак. К таким методам относится применение шифрования трафика, использование специальных методов согласования ключевой информации, контроль целостности канала и т.п. [3].

В последнее время ввиду падения эффективности MITM атак, а также их хорошей изученности злоумышленниками были разработаны новые классы атак MITB (в более широком смысле MITC). Этот класс атак характеризируется повышенной сложностью в сравнении с существующими MITM-атаками, а также, повышенной требовательностью к знаниям и навыкам разработчиков злонамеренного кода. Главной особенностью данного класса атак, является многоэтапность проведения

атаки на конечную систему для достижения поставленной цели разнесенная во времени. Информационная атака в общем случае может состоять из трех этапов [4]:

1. Сбор информации;
2. Этап реализации атаки;
3. Этап дальнейшего развития атаки.

Особенность MITB-атаки

Для атак класса MITB указанные этапы информационной атаки реализуются в виде трех последовательных фаз, которые следуют одна за другой:

1. Внедрение злонамеренного кода на удаленную систему/клиент.
2. Контроль информационных потоков на удаленной системе/клиенте с целью выявления целевых для атакуемой информационной системы.
3. Проведение направленной атаки.

Следует отметить, что проведения первой фазы атаки и оставшихся двух абсолютно независимы во времени, то есть внедрения злонамеренного ПО может быть значительно разнесено во времени и не иметь никаких априорных корелирующихся связей с последующей атакой и компрометацией целевой системы или клиентского устройства [5].

Этап внедрения злонамеренного кода на конечную систему пользователя предполагает получения как минимум тех же прав доступа и системных ресурсов, которыми обладает, атакуемо ПО [6]. Таким образом, достигается главная цель первой фазы атаки – получения полноправного доступа к обрабатываемой системой информации с максимальным затруднением обнаружения стороннего вмешательства. В существующих системах применяется базовая аксиома, что сама система защиты начинает функционировать в среде, которой можно заведомо доверять [7]. Исходя из этого, успешное достижении целей, которые преследует первая фаза атаки, позволяет полностью скомпрометировать используемую систему защиты таким образом, что она не имеет возможности обнаружить любой факт несанкционированных изменений данных со стороны постороннего ПО. Зачастую, кроме атаки на систему защиты конкретного приложения используемого для функционирования информационной системы, проводится компрометация общесистемных подсистем защиты, что позволяет эффективно внедрять любые злонамеренные модули ПО, вплоть до уровня ядра операционной системы, низкоуровневого драйвера устройства (например клавиатуры, мыши) и т.п.

Таким образом, это позволяет обходить любые существующие программные механизмы защиты, как на уровне операционной системы, так и на уровне конкретного атакуемого приложения, что позволяет достаточно просто скомпрометировать архитектурные методы защиты, такие как криптографические протоколы согласования ключей, параметров без необходимости проведения полномасштабных атак на алгоритмы шифрования или их конкретные реализации.

Следующей фазой атаки является пассивная фаза прослушивания и контроля информационных потоков, которые обрабатываются конечной системой пользователя. Эта фаза непосредственно относится к проводимой атаке.

Главными целями на этом этапе является прослушивание всех информационных потоков, которые могут быть созданы атакуемой информационной системой для выявления факта её использования. Также необходимо обеспечить максимальную скрытность в атакуемой системе для того что бы увеличить эффективность проводимой атаки за счет увеличения времени отслеживания активности пользователя. Это связано с той особенностью, что зачастую пользователь использует любую информационную систему периодически, возможно с большими временными интервалами. Таким образом, эффективность проводимой атаки напрямую зависит от времени, которое злонамеренное ПО находится в системе до момента его выявления и удаления.

Финальной фазой всего процесса является проведение целевой атаки на выбранную информационную систему (рис.2). Описанная схема функционирует следующим образом во время проведения первой фазы атаки на атакуемую систему устанавливается злонамеренное ПО. Это ПО внедряется в операционную систему на уровень ядра и перехватывает набор стандартных *API* вызовов ОС с помощью различных известных техник. После чего при вызове некоторой ФЗШ функции клиентским ПО этот вызов передается в ядро ОС не напрямую, а через злонамеренное ПО как показано на рис. 2. Таким образом, эти вызовы, проходя через злонамеренное ПО, могут анализироваться и модифицироваться нужным

злоумышленнику способом. Это позволяет скрывать присутствие злонамеренного ПО в системе клиента, а также эффективно проводить атаки, на целевое клиентское ПО. Дополнительно это ПО устанавливает скрытый канал связи, с вычислительным устройством злоумышленника используя при этом существующий физический канал связи атакованного вычислительного устройства.

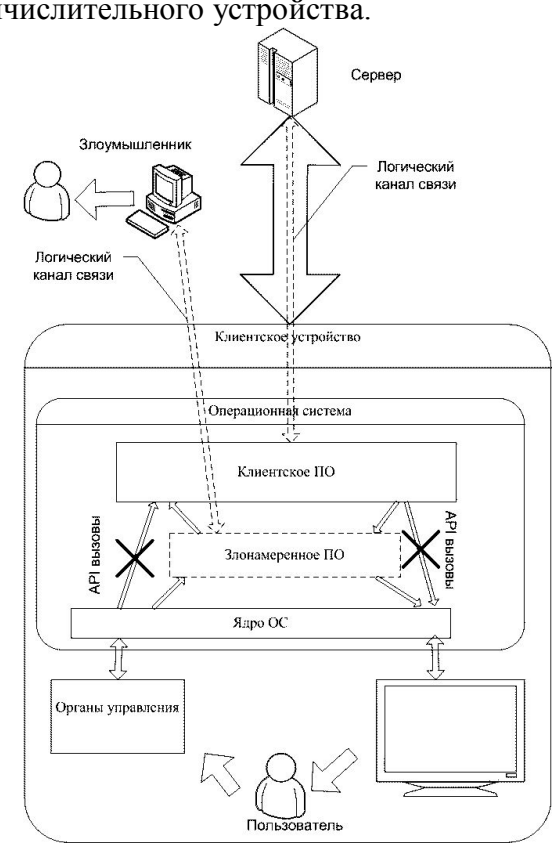

Рис.2. Схема проведения активной MITB атаки

На сегодняшний день разработано множество типичных схем проведения атак [8], которые с небольшой доработкой могут применяться для проведения успешных атак на различные сервисы которые обрабатывают «чувствительные» данные.

Направленная атака может быть или активной или пассивной в зависимости от целей, которые она преследует.

Пассивная атака предполагает, что после внедрения злонамеренного ПО на атакуемую информационную систему начинается вторая фаза проведения атаки. Во время проведения этой фазы производятся попытки обнаружить факты использования целевой информационной системы (нужный клиент-банк, заданная почтовая система и т.п.). В случаи успешного обнаружения подобного ПО производится запись данных, которые вводит и получает пользователь с его помощью. К таким данным относятся логин и пароль для аутентификации, введённые адреса получателей, различные «чувствительные» данные конкретного пользователя которые могут быть использованы в дальнейшем или проданы третьему лицу. Зачастую эти данные пересылаются на удаленный сервер злоумышленника с помощью построенного скрытого логического канала связи, где обрабатываются, и принимается решения о дальнейшем их использовании.

Основная трудность идентификации такой атаки с точки зрения защищающейся стороны заключается в том, что обнаружить и предотвратить каким-либо образом действия злоумышленника затруднительно, так как сам факт несанкционированного использования полученных данных будет обнаружен только после успешного проведения атаки. В основном украденные данные используются спустя несколько дней после фактически успешно проведенной атаки. Поэтому на атакованных клиентских устройствах уже может не быть самих модулей злонамеренного ПО, которое использовал злоумышленник, что значительно усложняет процесс проведения расследования и выявления причин и методов проведения успешного нападения.

Во время проведения активной атаки предполагается выполнение определенных действий направленных на модификацию или искажения передаваемых данных в режиме реального времени. Для этого с помощью перехваченных API функций ОС производится анализ данных, которыми обменивается атакуемая информационная система с различными подсистемами ОС (например драйвера органов управления, драйвер видеокарты и т.п.). И в случаи необходимости производится модификация передаваемых данных. При этом атакованному ПО достаточно затруднительно обнаружить сам факт подмены и модификации полученных или отправленных данных так как нет доступных методов верификации и аутентификации подобной информации что связано с архитектурой современных ОС.

На этом этапе, зачастую, применяются следующие векторы атак [9]:

- межсайтовый скриптинг;
- обратный веб-шелл;
- clickjacking;
- отравление кеша;
- удаленное подключение файлов на стороне клиента;

- межсайтовая публикация.

Кроме указанных общеизвестных векторов атак используются специально разработанные, под заданную информационную систему, атаки которые учитывают различные особенности функционирования атакуемой информационной системы, а также алгоритмы организации информационного обмена между серверным и клиентским ПО.

Выводы

Таким образом, в последнее время активно развивается новый класс атаки MITB который направлен на компрометацию современных распределенных информационных систем обрабатывающих «чувствительные» даны пользователей. В связи с этим исследование и разработка новых перспективных методов и технологий защиты от подобного рода атак является ключевым направлением в современных исследованиях. Знание особенностей развития и проведения таких атак позволяет выявить характерные особенности, а также определить дальнейшие направления исследований.

Список литературы

1. *Gühring P.* Concepts against Man-in-the-Browser Attacks // www.cacert.at/svn/sourcerer/CAcert/SecureClient.pdf.

2. Mannan M., van Oorschot P.C. Security and Usability: The Gap in Real-World Online Banking // New Security Paradigms Workshop (NSPW'07). – New Hampshire, USA. – 2007. – P. 1–14.

3. Mannan Mohammad. Authentication and securing personal information in an untrusted Internet. Ph.D. – Carleton university. – 2009. – P. 218.

4. Сердюк В.А. Информационная безопасность автоматизированных систем предприятий // Бухгалтер и компьютер. – 2007. – № 1. – С. 104 – 107.

5. Shener O. Automated Generation and Analysis of Attack Graphs // Proceedings of the 2002 IEEE Symposium on Security and Privacy – Oakland, CA, USA, 2002. – P. 273 – 284.

6. Казимир В.В., Серая А.А. Метод построения моделей информационных атак // Математичні машини і системи. – 2010. – № 4. – С. 52–61.

7. Сердюк В. А. Разработка и исследование математических моделей защиты автоматизированных систем от информационных атак : Дис. канд. техн. наук : 05.13.19 . – М. – 2004. – 173 с.

8. Натров В.В. Классификация сетевых атак // Информационные технологии в управлении и моделировании: сб. докладов. – Белгород, 2005. – С. 128–132.

9. Kapil Singh, Alexander Moshchuk, Helen J. Wang, Wenke Lee. On the Incoherencies in Web Browser Access Control Policies // IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010. – P. 463–478.