МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»

Институт математики, механики и компьютерных наук им. И.И. Воровича

Кафедра информатики и вычислительного эксперимента

КУРСОВАЯ РАБОТА

на тему: «Выявление возможности организации скрытых каналов передачи данных из защищаемых сетей»

Выполнил:
Студент 3 курса, 8 группы Д.Ю. Проскурин

Проверил:
кем работает Гуфан Константин Юрьевич

Ростов-на-Дону
2017

Оглавление

Введение

На последний момент возрастает актуальность темы защиты данных от утечек.

Говоря об информационной безопасности, в настоящее время имеют в виду безопасность компьютерную. Действительно, информация, находящаяся на электронных носителях играет все большую роль в жизни современного общества. Уязвимость такой информации обусловлена целым рядом факторов: огромные объемы, многоточечность и возможная анонимность доступа, возможность "информационных диверсий". Все это делает задачу обеспечения защищенности информации, размещенной в компьютерной среде, гораздо более сложной проблемой, чем, скажем, сохранение тайны традиционной почтовой переписки.

Если говорить о безопасности информации, сохраняющейся на традиционных носителях (бумага, фотоотпечатки и т.п.), то ее сохранность достигается соблюдением мер физической защиты (т.е. защиты от несанкционированного проникновения в зону хранения носителей). Другие аспекты защиты такой информации связаны со стихийными бедствиями и техногенными катастрофами. Таким образом, понятие компьютерной информационной безопасности в целом является более широким по сравнению с информационной безопасностью относительно традиционных носителей.

Если говорить о различиях в подходах к решению проблемы информационной безопасности на различных уровнях (государственном, региональном, уровне одной организации), то такие различия просто не существуют. Подход к обеспечению безопасности Государственной автоматизированной системы "Выборы"не отличается от подхода к обеспечению безопасности локальной сети в маленькой фирме.

Потому жизненно необходимы методы защиты информации для любого человека, использующего компьютер. По этой причине практически любой пользователь ПК в мире так или иначе «подкован» в вопросах борьбы с вирусами, «троянскими конями» и другими вредоносными программами, а также личностями стоящими за их созданием и распространением — взломщиками, спамерами, крэкерами, вирусмэйкерами (создателями вирусов) и просто мошенниками, обманывающих людей в поисках наживы — корпоративной информации, стоящей н емалых денег.

Для решения данной проблемы были реализованы средства предотвращения утечек информации, реализующих систему защиты данных от несанкционированного доступа к ней. Но злоумышленники придумывают новые способы заполучения информации. Поэтому важно проверять системы защиты на возможность кражи информации новыми методами

Цель: *Поиск недостатков существующих методов выявления скрытых каналов из защищаемых сетей*

Задачи:

1. Исследование и анализ известных DLP систем;
2. Разработать и реализовать методы обхода средств контроля исходящего сетевого трафика;
3. Развернут экспериментальный стенд;

4. Провести экспериментальные исследования, подтверждающие предположения о неэффективности современных средств защиты информации.

Глава 1

Современные системы защиты сетевого уровня.

1.1 Способы защиты информации

Для решения проблемы утечек данных обычно используют специальные технологии, предотвращающие возможность кражи данных из информационной системы. Эти системы получили название DLP (Data Leak Prevention, что переводится на русский как предотвращение утечек данных). Обычно под DLP-системами принимают некоторое программное обеспечение, предотвращающее потерю данных, путем обнаружения возможных нарушений доступа к конфиденциальной информации при ее передаче за пределы информационной системы. Как правило, большая часть утечек происходит благодаря человеческому фактору. Люди редко задумываются о безопасности своих действий. Этим и пользуются злоумышленники, пытающиеся получить конфиденциальную информацию некоторой фирмы. Как показывает статистика, лишь незначительная часть всех утечек происходит по злому умыслу работника или пользователя информационной системы.

Для борьбы с нежелательным копированием информации используются различные технологии. Условно их можно разделить на несколько категорий:

- стандартные меры безопасности;
- интеллектуальные (продвинутые) меры;
- контроль доступа и шифрование;
- специализированные системы DLP.

Стандартные меры безопасности

К таким мерам безопасности относится формирование Private Network (PN - частная сеть или локальная), которая позволяет создать внутреннюю сеть внутри информационной системы, не позволяя получить доступ к информации извне и из внутренней сети к глобальной сети. Таким образом можно достаточно надежно защитить данные, при условии, что сотрудники не станут копировать данные. Однако в современном мире активно используется сеть Интернет. Без нее уже трудно представить себе работу. А данный подход не предполагает доступ к всемирной паутине, иначе возникнет возможность утечки данных. Поэтому появилось расширение данной защиты — VPN (Virtual Private Network). Сеть также остается локальной, но существует некоторый сервер, через который пользователи получают доступ в Интернет, тем самым защищая себя от хакерских атак, которые возьмет на себя VPN сервер. Казалось бы все хорошо. Только нельзя забывать о вредоносном ПО, которое без проблем похитит все данные, попав на компьютер из глобальной сети. Обеспечив контроль трафика для

VPN, при которой сервер сам решает, пропускать ли ему тот или иной пакет в зависимости от выбранной политики безопасности, получаем следующую стандартную технологию защиты — Межсетевой экран (другие известные названия: сетевой экран Firewall, Брандмауэр). Для ее реализации используются специализированные программные обеспечения, которым задаются шаблоны зепрещенных соединений и правила обработки всего трафика. Однако и здесь есть проблемы с безопасностью данных. Те же самые вирусы уже давно научились передавать данные в зашифрованном или скрытом виде, применив методы стеганографии (это алгоритмы, позволяющие скрыть одну информацию в другой) . Обнаружить скрытую информацию достаточно тяжело и не всегда оказывается возможным, поэтому данную систему защиты в современном мире корректно настроить трудно.

К мерам стандартной безопасности также относят системы обнаружения вторжений (Intrusion Detection System). Это некоторое программное или аппаратное обеспечение, предназначенное для выявления неавторизованного доступа в информационную систему, в основном, через Интернет. Такие системы предназначены для обнаружения некоторых типов вредоносной активности, нарушающей безопасность системы. Обычно к такой активности относят сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

1.1.1 Антивирусное программное обеспечение

Одной из самой популярной системой системой защиты является антивирусное программное обеспечение, способное найти и обезвредить программы, наносящие вред компьютеру или информационной системе. В последнее время такие средства оказывают комплексную защиту от вирусов, помогая не только исправить проблему, но и предотвратить ее появление. Поэтому такие программные обеспечения обычно содержат в себе ранее описанные средства защиты, то есть VPN, IDS, межсетевой экран. Однако нужно понимать, что на самом деле антивирусы не способны найти все вредоносное ПО, которое попадет/попало на компьютер. Они всего лишь сравнивают поведение той или иной программы с поведением уже известных вирусов. Если программа не похожа ни на один популярный зловред, то антивирусы никак не реагируют. Но это не значит, что данная программа не является вирусом. К примеру, ориентировочно в 2011 году появился вирус ProjectSauron (Trojan.Multi.Remsec.gen), ворующий данные с зараженного компьютера. Основное его направление атак — правительственные компьютеры, на которых установлены различные системы защиты, включая антивирусы. Однако до сентября 2015 года ни один антивирус не считал его опасным.

1.1.2 Клиент-Серверная архитектура

Еще одной популярной системой защитой информации является организация клиент-серверной информационной системы. Такая архитектура предполагает хранение всей важной информации на защищенном сервере, обычно в виде базы данных, а все пользователи получают к ней доступ через специальные программы-клиенты, обычно передающие информацию в зашифрованном виде и не хранящие данные на компьютерах. Таким образом возможность утечки информации достаточна минимальна, но не исключает её.

Дополнительные меры безопасности используют узкоспециализированные сервисы и временные алгоритмы для обнаружения ненормального доступа к данным (т. е. к базам данных либо информационно-поисковых системам) или ненормального обмена электронной почтой. Кроме того, такие современные информационные технологии выявляют программы и запросы, поступающие с вредоносными намерениями, и осуществляют глубокие проверки компьютерных систем (например, распознавание нажатий клавиш или звуков динамика).

1.1.3 DLP системы

Для решения проблемы утечек информации реализовали специальные DLP системы, предназначенные для защиты информации и предотвращения попыток несанкционированного копирования и передачи конфиденциальной информации без разрешения или доступа со стороны пользователей, которые имеют право доступа к конфиденциальной информации.

Системы подобного рода строятся на анализе потоков исходящих данных, через которые может произойти несанкионированная передача важной информации. Если некоторая программа/пользователь пытается получить несанкционированный доступ к данным, которые защищены DLP, то такая система защиты срабатывает на попытку доступа, блокируя ее и сообщая администратору данной системы защиты.

Кроме основной перед DLP-системой могут стоять и вторичные (побочные) задачи. Обычно к ним относят:

- архивирование пересылаемых сообщений на случай возможных в будущем расследований инцидентов;
- предотвращение передачи вовне не только конфиденциальной, но и другой нежелательной информации (обидных выражений, спама, эротики, излишних объёмов данных и т.п.);
- предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы;
- предотвращение использования работниками казённых информационных ресурсов в личных целях;
- оптимизация загрузки каналов, экономия трафика;
- контроль присутствия работников на рабочем месте;
- отслеживание благонадёжности сотрудников, их политических взглядов, убеждений, сбор компромата.

1.2 Компоненты DLP

Выделяют три основных компонента DLP систем:

1. Network DLP
2. Endpoint DLP
3. Storage DLP

Network DLP

Данная система, как правило, представляет собой аппаратное решение или программное обеспечение, которое устанавливается в точках сети, исходящих вблизи периметра. Такая система анализирует сетевой трафик по любому каналу TCP/IP или UDP. Система контролирует обмен информацией через IM и пиринговые системы, а также позволяет блокировать пересылку информации через HTTP(s), FTP(s) и SMTP-каналы с возможностью информирования пользователей о нарушении корпоративной политики.

Endpoint DLP

Endpoint DLP производят контроль перемещения информации на устройствах. Позволяет в режиме реального времени отслеживать, а в случае обнаружения запрещенного контента —

и блокировать попытки копирования информации на съемные носители информации, печать и отсылку по факсу, по электронной почте и т. д.

Системы такого типа функционируют на рабочих станциях конечных пользователей или серверах в организациях. Конечная точка, как и в других сетевых системах, может быть обращена как к внутренним, так и к внешним связям и, следовательно, может использоваться для контроля потока информации между типами и группами пользователей. Прежде, чем данные сообщения будут загружены на устройство, они проверяются сервисом. При содержании неблагоприятного запроса сообщения будут заблокированы. Таким образом они становятся неоправленными и не попадают под действие правил хранения информации на устройстве.

Преимущество DLP системы заключается в том, что она может контролировать и управлять доступом к устройствам физического типа, а также получать доступ к информации до того, как она будет зашифрована. Некоторые системы, которые функционируют на основе конечных утечек, могут также обеспечить контроль приложений с целью блокировки попыток передачи конфиденциальной информации и обеспечения незамедлительной обратной связи с пользователем. Недостаток таких систем заключается в том, что они должны быть установлены на каждом устройстве и не могут использоваться на мобильных устройствах.

Storage DLP

Storage DLP производит контроль соблюдения процедур хранения конфиденциальных данных. Позволяет в режиме сканирования обнаруживать хранимые конфиденциальные данные на файловых, почтовых, Web-серверах, в системах документооборота, на серверах баз данных и т. д. Проводит анализ легитимности хранения данных в их текущем местонахождении и перенос при необходимости в защищенные хранилища.

1.3 Методы определения утечек

DLP система должна перехватывать все данные, передаваемые с данного устройства, и проверять их на наличие конфиденциальной информации. Задача анализа потока данных является нетривиальной, поскольку передается много разнообразной информации. В следствие этого поиск оказывается серьезно осложнен. Поэтому разработаны технологии для детектирования попыток передачи конфиденциальных данных.

Условно все способы обнаружения утечек можно разделить на две группы:

- анализ текстов передаваемых сообщений или документов
- поиск в данных специальных цифровых отпечатков, меток

1.3.1 Морфологический анализ

Данный метод ищет в потоке передаваемых данных заданные слова и словосочетания, поэтому он является одним из самых распространенных контентных способов обнаружения утечек конфиденциальной информации. Поскольку строгий поиск указанных выражений сам по себе бесполезен, то морфологический поиск должен учитывать все возможные формы заданных слов.

Главным преимуществом является его универсальность. С одной стороны, морфологический анализ может использоваться для контроля любых каналов связи, начиная с файлов, копируемых на съемные накопители, и заканчивая сообщениями в Skype, социальных сетях и пр. С другой – с его помощью могут исследоваться любые тексты и искаться любая информация. При этом конфиденциальные документы не нуждаются в какой-либо предварительной обработке. А защита начинает действовать сразу после включения правил обработки и распространяется на все заданные каналы связи.

Основным недостатком морфологического анализа является относительно низкая эффективность определения конфиденциальной информации. Причем зависит она как от используемых в системе защиты алгоритмов, так и от качества семантического ядра, применяющегося для описания защищаемых данных. Также немалое значение имеют и сами анализируемые тексты. Поэтому заранее предсказать степень эффективности обнаружения в передаваемом трафике конфиденциальных данных достаточно сложно. Увеличить ее можно точным подбором семантического ядра. При использовании морфологического анализа нужно учитывать риск ложного срабатывания системы защиты на вполне безобидные тексты. Его степень также зависит от семантического ядра и исследуемого трафика.

Несмотря на достаточно серьезные недостатки, морфологический анализ на сегодняшний день является единственно возможным методом обнаружения произвольной информации в любых текстах. Данный алгоритм постоянно совершенствуются, что повышает его точность.

В данных алгоритмах зачастую используются словари синонимов, которые позволяют увеличить эффективность морфологического анализа. Они значительно упрощают настройку морфологического анализа. Их использование позволяет при необходимости внесения корректировок в параметры защиты не редактировать вручную все правила, а только изменить состав нужного списка. При этом изменится работа всех правил, в которых используется данный словарь.

Кроме того, в некоторых DLP-решениях существует функция генерации семантического ядра. Она также основана на использовании словарей. Данная функция сканирует указанный набор документов, в ходе которого по специальному алгоритму выбираются слова и выражения, которые используются для описания текстов этого типа. Из них автоматически формируется словарь слов и словосочетаний защищаемых выражений.

1.3.2 Статистический анализ

Данный метод заключается в вероятностном анализе текста, который позволяет предположить его конфиденциальность или открытость. Для его работы обычно требуется предварительное обучение алгоритма. В ходе него вычисляется вероятность нахождения тех или иных слов, а также словосочетаний в конфиденциальных документах.

Преимуществом статистического анализа является его универсальность. При этом данная технология работает в штатном режиме только в рамках поддержания постоянного обучения алгоритма. К примеру, если в процессе обучения системе было предложено недостаточное количество защищаемой информации, то она не сможет определять факт их передачи. То есть качество работы статистического анализа зависит от корректности его настройки (обучения). При этом необходимо учитывать вероятностный характер данной технологии. Она только делает предположение, что анализируемый текст относится к разряду конфиденциальных.

1.3.3 Шаблоны

Во многих случаях конфиденциальная информация представляет собой некоторые стандартизованные данные, например, адреса, телефоны, серии и номера паспортов и пр. Для обнаружения попыток передачи такой информации существует специальный весьма эффективный метод – шаблоны.

Администратор, отвечающий за безопасность данных, определяет строковый шаблон конфиденциальных данных: количество символов и их тип (буква или цифра). После этого система начинает искать в анализируемых текстах сочетания, удовлетворяющие ему, и применять к найденным файлам или сообщениям указанные в правилах действия.

Главным преимуществом шаблонов является высокая эффективность обнаружения передачи конфиденциальной информации. Применительно к инцидентам случайных утечек она стремится к ста процентам. Однако злоумышленник, зная о возможностях используемой DLP-системы, может противодействовать ей, к примеру, разделяя символы различными символами.

К недостаткам шаблонов можно отнести ограниченную сферу их применения. Они могут использоваться только для стандартизованной информации, например, для защиты персональных данных. Еще одним минусом рассматриваемого метода является относительно высокая частота ложных срабатываний. Например, номер паспорта состоит из шести цифр. Но, если задать такой шаблон, то он будет срабатывать каждый раз, когда встретится шесть цифр подряд. А это может быть номер договора, отсылаемый клиенту, сумма и т. п.

В некоторых DLP-решениях технология шаблонов получила развитие, позволяющее нивелировать описанный выше недостаток. Достигается это за счет ее расширения дополнительными условиями: ключевыми суммами, диапазонами значений, словами, которые находятся неподалеку до или после найденной подстроки. При этом разработчики сами комплектуют поставку уже готовыми шаблонами со всеми необходимыми условиями, так что администратору безопасности остается при создании правила только выбрать нужные значения.

1.3.4 Цифровые отпечатки

Еще одной технологией обнаружения утечек конфиденциальной информации является технология так называемых цифровых отпечатков. С ее помощью можно с высокой степенью эффективности контролировать попытки передачи строго определенных документов или их фрагментов. Сначала создается специальная база «электронных слепков» с указанных администратором файлов. После этого все отправляемые документы будут проверяться на соответствие этим отпечаткам.

Под цифровым отпечатком в данном случае понимается целый набор характерных элементов документа, по которому его можно с высокой достоверностью определить в будущем. Современные DLP-решения способны детектировать не только целые файлы, но и их фрагменты. При этом можно даже рассчитать степень соответствия. Такие решения позволяют создавать дифференцированные правила, в которых описаны разные действия для разных процентов совпадения.

Важной особенностью цифровых отпечатков является то, что они могут использоваться не только для текстовых, но и для табличных документов, а также для изображений. Это открывает широкое поле для применения рассматриваемой технологии. Например, можно сделать цифровой отпечаток подписи главного бухгалтера, что позволит пресечь отправку всех отсканированных копий документов, им подписанных.

1.3.5 Цифровые метки

Данный метод основан на контроле действий над файлами, хранящими защищаемую информацию. На выбранные документы накладываются специальные метки, которые «видны» только клиентским модулям используемого DLP-решения. В зависимости от их наличия система разрешает или запрещает те или иные действия с файлами. Это позволяет не только предотвратить утечку конфиденциальных документов, но и ограничить работу с ними пользователей, что является преимуществом данной технологии.

К недостаткам относится ограниченность сферы ее применения. Защитить с ее помощью можно только текстовые документы, причем уже существующие. На вновь создаваемые документы это не распространяется. Частично этот недостаток нивелируется способами автоматического создания меток, например, на основе набора ключевых слов. Однако данный

аспект сводит технологию цифровых меток к технологии морфологического анализа, то есть, по сути, к дублированию технологий.

Другим недостатком технологии цифровых меток является легкость ее обхода. Достаточно вручную набрать текст документа в письме, и данный способ будет бессилен. Поэтому он хорош только в сочетании с другими методами защиты.

1.3.6 Инструменты противодействия обходу защиты

Все описанные выше технологии основаны на анализе обычного текста. Однако в некоторых случаях злоумышленники могут использовать различные методы обхода системы защиты, основанные на сокрытии этого текста. Самым простым из них является архивирование пересылаемых документов. Для защиты от этого в DLP-решениях обычно реализуется поддержка разных форматов сжатия. В этом случае файлы распаковываются, а их содержимое проверяется обычным образом. Поэтому в DLP-системе должна присутствовать возможность адекватной реакции на архивы, защищенные паролем. При обнаружении таких файлов они могут, например, перемещаться в карантин.

Следующий способ «спрятать» конфиденциальную информацию – транслитерация. Злоумышленник может взять текст и перевести все его символы на латинский алфавита. Для противодействия транслитерации конфиденциальной информации используется транслитерация заданного семантического ядра. При включении этой функции DLP-система проверяет тексты на наличие как обычно записанных слов, так и их «транслитерационных» аналогов. Причем в некоторых решениях правила преобразования можно задавать вручную.

Еще одним способом обхода DLP-системы является отправка текста в виде картинки (например, скриншот открытого документа). Для противодействия этому методу используются OCR-технологии. То есть система защиты пытается распознать все отправляемые изображения. В случае успеха выделенный текст обрабатывается по обычным правилам.

Глава 2

Каналы утечки информации

2.1 Определение

Утечку информации в общем плане можно рассматривать как неправомерный выход конфиденциальных сведений за пределы организации или круга лиц, которым эти сведения были доверены.

Утечка информации по своей сущности всегда предполагает противоправное (тайное или явное, осознанное или случайное) овладение конфиденциальной информацией, независимо от того, каким путем это достигается.

Утечку охраняемой информации, может произойти при наличии ряда обстоятельств. Если есть злоумышленник, который такой информацией интересуется и затрачивает определенные силы и средства для ее получения. И если есть условия, при которых он может рассчитывать на овладение интересующую его информацию (затратив на это меньше сил, чем если бы он добывал ее сам).

Что касается причин и условий утечки информации, то они, при всех своих различиях, имеют много общего.

Причины связаны, как правило, с несовершенством норм по хранению секретной информации, а также с нарушением этих норм (в том числе и несовершенных), отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и других материалов, содержащих конфиденциальную информацию.

2.2 Виды утечек

Утечка информации возможна по разным причинам, а именно:

- Умышленные утечки информации – это случаи преднамеренной утечки данных, когда пользователь, имеющий доступ к ценной информации, знал о возможных негативных последствиях своих действий, понимал, что такие действия носят противоправный характер. Кроме того, сотрудник организации получал предупреждение об ответственности, но все равно передавал данные или создавал условия для их утечки, желая получить материальное вознаграждение или иную выгоду для себя. В результате действий сотрудника возникли условия, способствующие потере контроля над информацией, нарушению конфиденциальности данных. При этом не имеет значения, были ли негативные последствия для компании или отдельных лиц от действий, совершенных инсайдером;

- Кража информации (извне). Взлом компьютера с помощью вредоносных программ и похищение информации с целью использования в корыстных интересах;

- Взлом программного обеспечения. На хакерские атаки приходится 15% от всей утечки информации. Вторжение в устройство извне и незаметная установка вредоносных программ позволяет хакерам полностью контролировать систему и получать доступ к закрытым сведениям, вплоть до паролей к банковским счетам и картам. Для вторжения извне в устройство могут применяться различные программы типа трояна. Главное отличие этого вида утечки – активные действия внешних лиц с целью доступа к информации;

- Кражи носителей. Достаточно распространенный способ утраты случается в результате преднамеренной кражи устройств с информацией. В большинстве случаев это случается из-за кражи ноутбуков, смартфонов, планшетов и других съемных носителей данных в виде флэшек, жестких дисков;

- Случайные утечки. К этому виду можно отнести веб-утечки, которые чаще всего происходят в силу неосведомленности или ошибочных действий сотрудников организации. Такой вид утраты случается в результате размещения конфиденциальной информации в интернет. Также, не последнюю роль играет человеческий фактор, когда сотрудник умышленно или без умысла позволяет получить доступ к закрытым данным всем желающим.

Рассмотр утечек, зависящие от человеческого фактора можно опустить, поскольку данные способы в большем случае не подвергаются контролю DLP систем и их почти невозможно контролировать. Данные системы в большей части отслеживают все каналы, через которые возможно передавать информацию. Подобным функционалом обладает Firewall, который лежит в основе каждой DLP системы и обладающий дополнительными возможностями.

В настоящий момент существует множество протоколов, через которые можно передавать данные. Данное условие сильно усложняет работу межсетевым экранам.

2.3 Каналы утечек

Для организации каналов передачи данных злоумышленники могут использовать различные протоколы, в том числе и служебные. Рассмотрм некоторые из них.

2.3.1 HTTP Get и Post - запросы

HTTP (HyperText Transfer Protocol — "протокол передачи гипертекста").

В компьютерной терминологии, гипертекст — текст, сформированный с помощью языка разметки, потенциально содержащий в себе гиперссылки, то есть ссылки на другой элемент в самом документе, а также на другой объект, расположенный на локальном диске или в компьютерной сети, либо на элементы этого обьекта.

Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

Данный протокол в последнее время получил широкое применение для обмена информацией между клиентом и сервером. С помощью POST, GET и HEAD HTTP запросов пользователь может предать необходимые данные на сервер. Данный протокол является простым в использовании и реализации, что его делает популярным каналом для передачи информации на удаленный сервер, используемым в вредоносных программах, самыми извеспными из которых являются Carberp (POST, GET), SpyEye (POST), Storm, ZeuS (POST, GET).

Отличительным средством данного протокола является скрытие настоящего сервера, принимающего и обрабатывающего информацию. Данная функция основывается на использовании Http-Proxy сервера, который подменяет собой скрываемый сервер и сам выполняет запрос к нужному компьютеру, передавая данные от клиента. Данная функция была введена в глобальную сеть из-за просчетов при создании стандарта TCP/IP. Данный стандарт создавался во время малочисленных компьютеров, которые в основном принадлежали крупным университетам, и предполагал, что у каждого компьютера будет свой адрес, однозначно идентифицирующий его. Но прогресс не стоит на месте. В скором времени таких адресов стало резко не хватать (что происходит и по сей день). Самым простым решением данной проблемы стало введение Proxy-серверов, которые в последующее время незначительно изменились и получили название NAT («транслятор сетевых адресов»). Но оригинальные Proxy сервера существуют и по сей день. Ими и пользуются злоумышленники для своих программ (например Wirenet).

2.3.2 Почтовые сервера

В 1960-х годах использовались различные виды электронной связи. Люди связывались друг с другом с помощью систем, разработанных для мейнфреймов. Когда всё больше компьютеров становились связанными ARPANET, были разработаны стандарты для того, чтобы пользователи на различных системах могли писать электронные сообщения друг другу. Эти стандарты, разработанные в 1970-х годах, стали основой для SMTP.

SMTP стал широко использоваться в ранние 1980-е. В то время он был дополнением для работающей под Unix почтовой программы Unix Copy Program (UUCP), которая больше подходила для обработки передачи электронных сообщений между периодически связанными устройствами. С другой стороны, SMTP прекрасно работает, когда как отправляющее, так и принимающее устройства связаны в сети постоянно. Оба устройства используют механизм хранения и пересылки и являются примером push-технологии.

Предоставление сообщений (RFC 2476) и SMTP-AUTH (RFC 2554) были введены в 1998 и 1999 гг. и описывали новые тенденции в передаче электронных сообщений. Изначально, SMTP-сервера были обычно внутренними для организации, получая сообщения от организаций извне и ретранслируя сообщения организации во внешнюю среду. Но с течением времени, SMTP-сервера расширяли свои функции и в стали агентами предоставления сообщений для пользовательских почтовых приложений, некоторые из которых теперь ретранслировали почту извне организации.

На практике данный протокол не получил такую популярность среди вредоносных программ как HTTP. Но несмотря на это некоторые приложения, например Sality или ProjectSauron, используют именно его для обмена информацией с управляющим сервером.

2.3.3 DNS - Domain Name System

Каждый компьютер в Интернете имеет свой IP-адрес – 4 числа от 0 до 255. Такой адрес удобен при маршрутизации, так как определяет месторасположение компьютера в сети Интернет. Однако, такие числа неудобны для восприятия пользователем и вызывают проблемы при смене IP адреса у компьютера.

В сети ARPANET соответствие между текстовыми и двоичными адресами записывалось в файле host.txt, в котором перечислялись все хосты и их IP-адреса. Каждую ночь все хосты получали этот файл с сервера, на котором он хранился. В сети, состоящей из нескольких сотен устройств, работающих под управлением системы с разделением времени, такой подход работал вполне приемлемо.

На смену «однофайловой» схеме пришел DNS, являющийся иерархической схемой имен,

основанной на доменах, и распределенной базе данных. В первую очередь эта система используется для преобразования имен хостов и пунктов назначения электронной почты в IP-адреса, но также может использоваться и в других целях.

Данный протокол на данный момент только набирает популярность среди разработчиков вредоносных программ. С помощью него функционируют вредоносные программные обеспечения, такие как ProjectSauron и Multigrain.

Глава 3

Анализ надежности DLP систем

При создании экспериментального стенда использовался COMODO Firewall, который оснащен функциями DLP системы. На данной системе защиты информации были проверены следующие методы построения скрытых каналов:

- передача данных с помощью POST запроса с использованием/без использования Proxy
- подмена host-файла
- Передача данных через почтовый сервер
- передача данных через Google Forms
- DNS - канал передачи данных
- передача данных через поисковые системы

3.1 Использование POST запроса с использованием Proxy

Интернет — всемирная система объединенных компьютерных сетей, построенная на базе IP и маршрутизации IP-пакетов. Интернет образует глобальное информационное пространство, служит физической основой для Всемирной паутины, изначально создававшейся как глобальная библиотека, позволяющая только передавать клиентам документы в электронном виде. Однако этого было не достаточно. Интернет-ресурсам требовался обмен информации, при котором клиент мог отправить данные на HTTP сервер. Для этой цели был разработан протокол Get. Данный стандарт сильно ускорил развитие интернета, однако он имеет некоторые недостатки, которые исправил протокол Post.

Поскольку, используя данные средства можно передавать данные на удаленный сервер, то возникло предположение, что подобным способом можно организовать скрытую перечу информации незаметно для DLP системы.

Реализация данного метода оказалось примитивной. Потребовалось организовать Http сервер и реализовать программу, передающую данные через Get/Post.

Тестирование данного метода было успешным. Однако в каждой DLP системе встроен firewall, способный детектировать соединения недостоверных программ к ненадежным ресурсам. В данном случае COMODO не справился с данной задачей и позволил передать данные. Но в общем случае данный способ не должен работать. Кроме того в каждый firewall встроен список вредоносных ресурсов, который он постоянно обновляет. Если ресурс попадет в этот список, то система защиты не позволит подключиться к данному серверу. Поэтому данный канал является ненадежным. Было предположено, что для обхода данной защиты

можно воспользоваться Proxy-сервером, который возьмет на себя организацию подключения к вредоносному ресурсу.

Прокси-серверы появились на заре эпохи Интернета, когда пользователей этой сети становилось все больше и больше, а внешние IP-адреса стоили немалых денег. Тогда основным назначением proxy-серверов являлась организация доступа в Интернет локальных пользователей без добавления их компьютеров к Глобальной сети, то есть без назначения внешних IP-адресов компьютерам, а выход в Интернет осуществлялся только с одного внешнего IP-адреса. Слово proxy в переводе с английского означает «доверенное лицо» или «представитель». Условно говоря, прокси-сервер действует от лица клиента в Интернете, и для других пользователей Сети виден только сам сервер, а не клиент. Таким образом, кроме общего доступа в Интернет локальных пользователей, которые не имеют прямого выхода в Сеть, такие серверы позволяют соблюсти приватность работы в Интернете. Вследствие того, что компьютеры обычных пользователей не размещены непосредственно в Сети, снижается угроза хакерских атак, поскольку прямого доступа к компьютерам локальной сети нет.

Существует несколько типов прокси-серверов, каждый из которых имеет узкую специализацию, то есть поддерживает работу только с одним или несколькими протоколами. Самыми распространенными на данный момент являются http-, Socks- и NAT-прокси. Последние входят в стандартные компоненты современных операционных систем, таких как Linux и Windows. По своим характеристикам программные прокси-серверы NAT практически не отличаются от аппаратных (маршрутизаторов) и существенно уступают в администрировании узкоспециализированным прокси-серверам.

Организовав Proxy-сервер на базе 3Proxy, была произведена незначительная модификация программы и проведено повторное тестирование, которое показало, что DLP не смогло предотвратить соединение данной программы к прокси-серверу, что позволило передать данные. COMODO в данном случае также не смог предотвратить недостоверное соединение, передающее защищаемые данные.

3.2 Подмена host файла

Самым простым способом организации доменов являлся файл host, позволяющий сопоставлять имена с IP адресами компьютеров на уровне операционной системы. Данный способ также был неудобен для использования обычными пользователями сети, но он дал основу для организации более совершенных систем, включая DNS.

Не смотря на свой возраст данный файл до сих пор используется в каждой операционной системе для организации технического DNS, используемого для отладки оборудования и программных средств.

Воспользовавшись данной информацией, была выдвинута гипотеза, что исправить недостаток предыдущего метода (использование POST запроса с Proxy) можно, модифицировав данный файл, добавив в него домен легетимного сайта, указывающего на сервер, принимающий информацию от нашей программы, знающей об этой модификации.

Реализация данного метода потребовала незначительной модификации программы из предыдущего метода передачи данных, добавив в нее редактирование файла host.

При проведении эксперимента COMODO Firewall сразу заметил попытку изменения системного файла host и заблокировал ее. При дальнейшем анализе было выяснено, что данная DLP система заставляет игнорировать операционную систему данный файл, что не позволяет организовать канал передачи данных таким образом.

3.3 Использование почтового сервера

На данный момент электронная почта очень активно используется в бизнес-среде, так как она представляет собой уникальную среду общения, которая может использоваться в качестве оперативного и очень недорогого средства для связи как между сотрудниками компании, так и с партнерами и клиентами. Правда, для того, чтобы ее использование получило максимальную эффективность, компании необходимо организовать собственный почтовый сервер. Только в этом случае корпоративная почта становится легко управляемым, безопасным, а также наиболее удобным и дешевым в применении бизнес-инструментом.

Подобная информация натолкнула на еще один способ организации скрытого канала, основанного на том, что вредоносная программа может заполучить данные для доступа к данному почтовому серверу и воспользоваться им для передачи информации, прикрываясь одним из сотрудников, чьи данные удалось заполучить программе.

При анализе данного способа построения скрытого канала не учитывалась возможность получения данных клиента почтового сервера. Предполагалось, что злоумышленник может просканировать приложения, установленные на компьютере, выделить среди них почтовые приложения и получить данные авторизации. Поэтому в ходе эксперимента использовался локальный SMTP сервер, через который передавались данные.

Таким образом, при реализации данного канала был зарегистрирован тестовый адрес электронной почты, на который производилась отправка данных, была реализована программа, подключающаяся к SMTP серверу и передающая через него электронные письма, был запущен Softstack SMTP сервер на тестовом компьютере.

В ходе эксперимента COMODO никаким образом не предотвратил передачу информации через локальный почтовый сервер и установление скрытого канала передачи данных было успешным. Однако следует учесть, что некоторые DLP системы не позволяют передавать электронные письма без разрешения на то администратора или подробно не изучив содержимое электронного письма..

3.4 Использование средств Google

Интернет со времени его возникновения сильно изменился. Он превратился из службы доставки документов в сервис доставки веб-приложений, предоставляющих различный функционал для пользователя будь то обмен сообщений между пользователями или вычисление сложных математических выражений. Интернет превратился в распределенную систему, каждое звено которой выполняет свою роль. Среди всех этих ресурсов можно выделить легетимные сервисы, облегчающие выполнение поставленной задачи. Зачастую такими сервисами пользуются злоумышленники, поскольку такие ресурсы зачастую сетевые экраны не проверяют, а у системного администратора, отвечающего за безопасность сети, обращение к ним не вызовет интереса.

Одним из таких ресурсов является Google Forms, позволяющий создавать публичные опросы и анкеты. Данный сервис получил огромную популярность среди тех, кто проводить сбор данных.

Возникло предположение, что воспользовавшись данным сервисов не по на значению, можно передавать данные от зараженного компьютера к злоумышленнику в обход DLP систем, тем самым организовав скрытый канал передачи данных.

Для реализации данного метода потребовалось зарегистрировать в системе Google Forms анкету с полями для приема данных. Проанализировав исходный код полученного опросника, выделил из него параметры POST запроса, использующие для передачи информации системе. Далее реализовал программу, обращающуюся к Google Forms и передающую ей

POST запрос, содержащий защищаемую информацию, защищенную шифрованием методом сдвига.

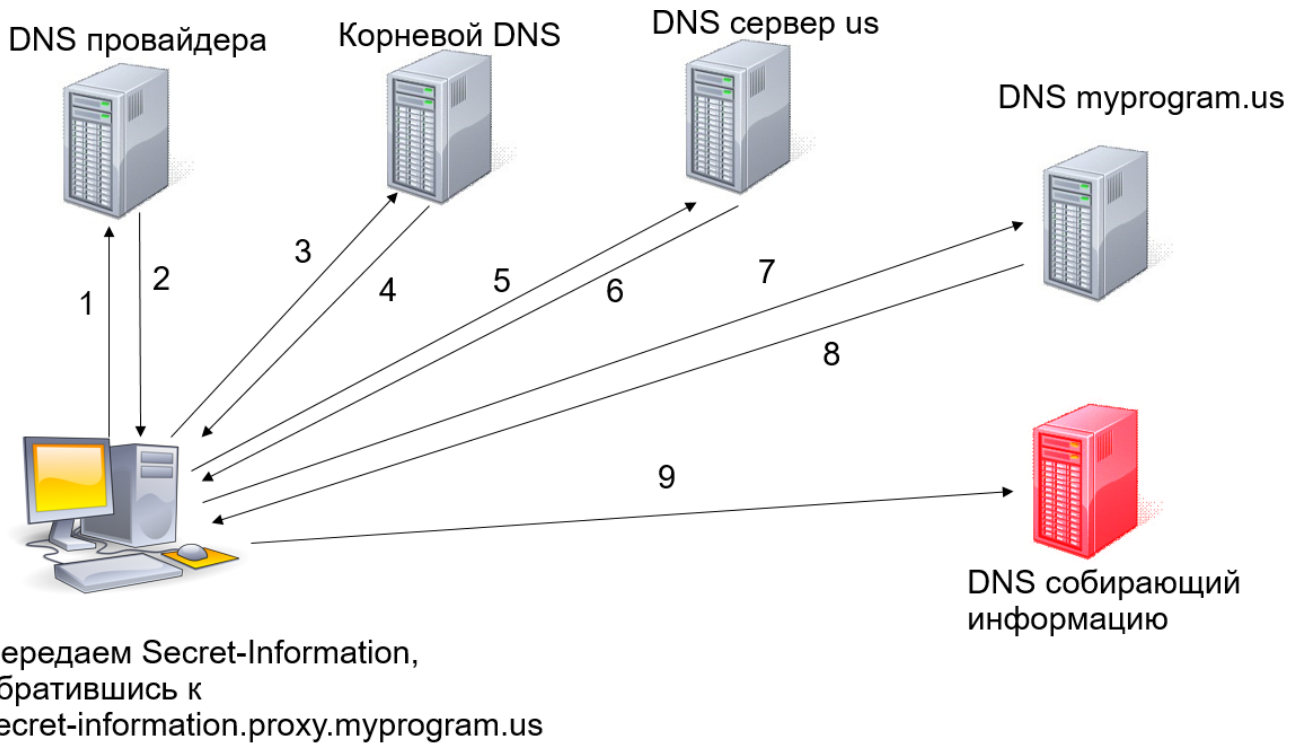
На практике COMODO сразу заметил, что недостоверная программа обращается к легитимному сайту, защищенному SSL сертификатом, о чем DLP доложила администратору сети. Если опустить данный факт из внимания, то данный канал является работоспособным и подобным образом можно реализовать канал передачи данных, который DLP системы могут не обнаружить.

3.5 Использование системных служебных функций DNS

Для поддержания работы сети Интернет были введены служебные протоколы, к которым относится DNS. Данный протокол позволяет по доменному имени получить IP адрес сервера, отвечающего за работу данного сайта. Для этого требуется выполнить несколько запросов к DNS серверам. Они начинаются с анализа файла host, а затем происходит обращение к серверу провайдера, корневым серверам, серверам зоны... Поскольку количество запросов отправляемые к серверам велико, то для обеспечения быстродействия работы через интернет системы защиты информации часто не проверяют сервера, на которые передают запрос, на недостоверность. Данную ситуацию сильно усугубляет существование DNS серверов, способные выполнять рекурсивные запросы.

Проанализировав данный протокол возникло предположение, что возможно построить с помощью него скрытый канал передачи информации, скомпрометировав DNS нескольких доменов и используя их субдомены как средство передачи данных.

При реализации было учтено, что злоумышленник может использовать не только скомпрометированные сервера, но и свои с установленными на них соответствующих программ. Поэтому был создан сервер с установленным на нем программного обеспечением Bind, позволяющим организовать DNS сервер, который был настроен так, что все запросы, адресованные к нему, обрабатывались и сохранялись. Также был зарегистрирован домен proxy.myprogram.us, который был привязан к созданному серверу. Разработано программное обеспечение, которое всю информацию, передаваемую через DNS канал, шифровало методом сдвига, разбивало на порции по 50 символов и полученные строки интерпретировало как субдомены домена proxy.myprogram.us и выполняло DNS запрос. Таким образом был получен канал передачи информации через протокол системного уровня — DNS.



Тестирование данного канала с работающей DLP системой было успешным. Comodo Firefall не смог обнаружить этот скрытый канал и данные были переданы на удаленный сервер.

3.6 Использование поисковых систем для передачи информации

Во времена, когда только начиналось развитие интернета, объём доступной информации был сравнительно мал, и пользователей сети было немного. На начальных стадиях развития сети, ее использовали сотрудники университетов и исследовательских лабораторий для обмена информацией между учреждениями.

Первым способом организации и систематизации доступа к информационным ресурсам стало создание каталогов сайтов. В них стали группировать ссылки согласно определенной тематике.

С течением времени интернет набирал популярность и количество сайтов в нем росло быстрыми темпами и каталоги разрастались с неимоверной скоростью. Кроме того данный способ структурирования интернет-ресурсов был не удобен в поиске конкретной информации, поскольку предоставлял доступ только к списку сайтов, а не их содержимого.

В 1994 году появилась первая поисковая система WebCrawler, которая позволяла искать по интернет-ресурсам требуемую информацию и выводила ее пользователям на экран.

До сих пор поисковые системы не утратили своей актуальности. С каждым днем появляются десятки новых сайтов. Для удобства управления своими ресурсами данные системы ввели средства «Вебмастера», позволяющие получить информацию об индексировании сайта и поисковых запросов к нему.

Возникает предположение, что через данные легетимные поисковые системы можно организовать скрытый канал передачи информации, используя средства «Веб-мастера» и функцию «Поиск для сайта», предоставляемую почти каждой поисковой системой.

При реализации данного канала в поисковой системе Яндекс был зарегистрирован сайт proxy.myprogram.us и была подключена к нему услуга «Поиск для сайта», предоставившая уникальную ссылку на поисковую систему, из результатов поиска которой исключались все

ресурсы, кроме proxy.myprogram.us. Для передачи информации разработано программное обеспечение, которое всю, передаваемую через данный канал, шифровало методом сдвига, разбивало на порции по 100 символов и полученные строки интерпретировало как поисковый запрос к поисковой системе Яндекс.

Тестирование данного канала имело бы успех, если бы DLP система не детектировала попытку установления защищенного соединения через SSL с поисковой системой. Firewall не блокировал соединение, но выдавал предупреждение администратору системы о том, что неизвестная программа пытается установить соединение с поисковой системой. Если не обращать на данное предупреждение внимание, то в остальном передача информации через поисковую систему Яндекс была успешной.

Заключение

Из всего вышесказанного можно сделать выводы:

- Для передачи информации из защищаемых сетей могут использоваться служебные протоколы передачи данных, анализ которых может быть отключен по-умолчанию.
- Для обнаружения утечек информации недостаточно детектировать соединения на недоверенные ресурсы.
- Поиск в передаваемых данных защищаемой информации не гарантирует отсутствие канала её утечки, даже через поисковые запросы.
- Высокую эффективность в анализе безопасности защищаемых сетей показывают тесты на проникновение.

Дальнейший интерес представляют исследования:

- Создание средств обнаружения угроз по выявлению скрытых каналов.
- Поиск иных каналов утечки информации в обход современных DLP - систем

Литература

[1] *Ю. Н. Зиганайлов* Теория информационной безопасности и методология защиты информации Издательство: Москва-Берлин 2015.

[2] *К. Е. Климентьев* Компьютерные вирусы и антивирусы: взгляд прогаммиста Издательство: ДМК

[3] *Стив Макконнелл* Совершенный код. Издательство: Питер.

[4] *Б. Анин* Защита компьютерной информации. Издательство: БХВ-Петербург, 2000

[5] Исследование каналов, используемые вирусами производилось с помощью интернет-ресурсов securelist.ru, www.anti-malware.ru и xakep.ru