

УДК 003.26.7 004.9

О подходах к обнаружению прослушивания трафика в анонимной сети Тор

***Жилина В.С., студентка**
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»*

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

***Работаев Н.М., студентка**
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»*

***Работаев И.М., 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»*

tompetrov@yandex.ru

Задача выявления подслушивания трафика в сети затрудняется тем, что подслушивание – полностью пассивный процесс, не проявляющийся в системе каким-либо образом. В качестве одного из возможных путей преодоления этого затруднения предлагается провоцировать подслушивающего агента на активные действия, например, на переход к использованию перехваченных данных.

В статье описывается использование подставных сообщений для обнаружения перехвата трафика в анонимных системах с проксированием. Подход основывался на вставке в текущий трафик подложных сообщений с реквизитами для идентификации пользователей на подложных серверах. Конечной целью было обнаружение подслушивания путем выявления обращений с перехваченными реквизитами к контролируемым серверам-ловушкам.

Интернет-пользователи часто доверяют системам, не находящимся непосредственно под их контролем. С появлением облачных вычислений и постоянно увеличивающимся числом сервисов, перенесенных в облако, эта ситуация возникает все чаще. Такими системами являются анонимные и конфиденциальные сети Tor, Anonymizer, и многие другие. Они направляют трафик пользователя через один или несколько прокси-сервер, часто используя многослойные схемы шифрования, и достигают двойную цель. Во-первых, сохраняют анонимность пользователя, а во-вторых, они предоставляют пользователям сервисы и данные, которые могут быть ограничены по доступу. Например, анонимные сети позволяют пользователям избегать отслеживания провайдерами и государственными органами при обращении к данным ограниченного доступа.

Пользователи анонимных сетей могут скрывать такую информацию, как IP адрес, от провайдера конечного сервиса. Вместо этого, они вынуждены доверять компонентам используемых анонимных сетей. Во всех случаях, данные пользователя в некоторой точке (например, перед передачей на конечный сервис) доступны в первичном виде. Даже если шифрование используется внутри системы, окончательное шифрование обязательно для обеспечения конфиденциальности обмена данными пользователя. Это может привести к раскрытию конфиденциальной информации пользователя таким вредоносным элементам сети, как промежуточные ISP маршрутизаторы или узлы анонимных сетей, которые могут легко перехватывать трафик пользователя.

Корпоративные и иногда даже национальные сети блокируют доступ к социальным сетям и другим популярным онлайн-сервисам по разным причинам. Из-за этого пользователи часто обращаются к распределенным системам проксирования (как обеспечивающих анонимность, так и другим) для предотвращения фильтрации трафика. Многие из них не осознают различия между анонимностью и гарантиями конфиденциальности, предлагаемыми этими системами, и недостаточной конфиденциальностью, и пользуются ими при отсутствии окончательного шифрования, раскрывая свои данные прокси-серверам, передающим трафик пользователей. Некоторые сервера могут быть вредоносными и перехватывать такую личную информацию пользователя как логины и пароли или параметры для входа для несанкционированного использования.

Эта проблема не решается полностью с помощью окончательного шифрования. Злоумышленники из числа операторов связи, например, могут использовать атаки посредников и перехватывать трафик даже зашифрованных SSL сессий. Более того, хотя аутентификация пользователей производится с помощью HTTPS, многие сайты

переключаются на простой HTTP до окончания пользовательской сессии, позволяя осуществить hijacking атаку и перехватить сессию пользователя. Так поступают популярные сайты facebook.com и twitter.com, которые используют шифрование для аутентификации пользователя, но переключают аутентифицированные сессии на текстовый обмен, несмотря на то, что пользователь выбрал постоянный HTTPS доступ. Это особенно важно, учитывая, что более 50% HTTP трафика, посылаемого через выходные узлы Tor, уходит в социальные сети.

В ходе проведенного исследования рассматривался метод использования подложных сообщений для обнаружения перехвата в сетях с прокси, и в частности в анонимных сетях. Создатели данного метода выкладывали подставные реквизиты для различных сервисов, таких как SMTP, в анонимной сети Tor, и использовали их для обнаружения выходных узлов, на которых перехватывался пользовательский трафик. Использование подложной информации или данных-приманок для обнаружения неавторизованного использования конфиденциальных данных давно известно. Подложная информация использовалась ранее для определения подслушивания в незащищенных беспроводных сетях против угрозы проникновения. Идея состоит в том, что злоумышленники возможно будут использовать полученную информацию. Добавляя к трафику данные для аутентификации на контролируемых сервисах, можно обнаружить использование подложных логинов и паролей и отследить их до выходного узла сети Tor, на котором они были перехвачены.

Tor – одна из самых популярных анонимных сетей, основанная на «луковой» маршрутизации. Клиенты сети Tor формируют виртуальные соединения, состоящие из двух или более узлов, которые передают трафик пользователя на конечный сервер. Их данные шифруются несколько раз перед передачей через сеть Tor таким образом, чтобы исходная информация была доступна только на выходном узле (последнем узле в маршруте). Несмотря на то, что используется окончное шифрование между клиентом и сервером, конфиденциальность может оказаться под угрозой. Например, данные могут быть перехвачены с помощью вредоносного или зараженного выходного узла или даже ISP на выходном узле. На самом деле, все системы с прокси сталкиваются с одной и той же угрозой, если не используется окончное шифрование. Проверка системы обнаружения производилась в сети Tor, в основном потому, что Tor – самая популярная анонимная сеть с обширной базой пользователей и сотней выходных узлов, которые смогут быть использованы с любым TCP-сервисом, включая те, которые не используют окончное шифрование.

Система использует подложные реквизиты для контролируемых IMAP и SMTP серверов. Они передаются в текстовом виде, и каждое сообщение передается через один выходной узел, позволяя связать каждое конкретное сообщение с выходным узлом. Подставные реквизиты изображают правдоподобные пользовательские сессии, содержащие много взаимодействий клиент-сервер, так что подложный трафик становится практически неотличимым от настоящей пользовательской сессии. Система работала около десяти месяцев и обнаружила за это время десять случаев перехвата на общедоступных узлах сети Tor. По данным был создан прототип системы анонимной сети Tor, который находится в постоянной эксплуатации с августа 2010 года. Наблюдаемые инциденты подслушивания были связаны с десятью различными выходными узлами, и все незаконные подключения были получены IMAP сервером-ловушкой. На основании перехваченных учетных данных, используемых в каждой нежелательной связи, можно определить выходной узел Tor, участвующий в каждой аварии.

Первые четыре инцидента произошли в течение короткого промежутка времени (трех дней), и были задействованы четыре различных выходных узла в США, Гонконге, Великобритании и Нидерландах. Попытки подключения обратно на сервер-ловушку были схожи, и во всех четырех случаях они произошли от того же IP-адреса выходного узла. Еще одно сходство между этими инцидентами связано с разницей во времени между последним появлением подставных сообщений в сети и соответствующим соединением обратно на сервер-ловушку. Первые четыре инцидента имели довольно похожие задержки подключений через несколько часов, что значительно короче по сравнению с остальными инцидентами. На основании вышеизложенных фактов, предполагается, что первые четыре случая подслушивания были скоординированы одним и тем же лицом или группой, которые, вероятно, использовали одинаковые инструменты или методы в каждом случае.

Пятый инцидент произошел через три недели после предыдущих. Подставные логин и пароль были переданы через выходной маршрутизатор в Южной Корее, и была предпринята попытка подключения к серверу-ловушке с другого маршрутизатора в США - это признак того, что преступник, вероятно, использовал Tor, чтобы скрыть подлинное происхождение соединения. Шестой инцидент почти полностью совпал с пятым, но участвовал маршрутизатор в Гонконге. После более чем десяти часов, сервер IMAP получил шесть соединений с другого IP адреса, принадлежащего китайскому провайдеру.

В седьмом случае подслушивания учетные данные пользователей были переданы через маршрутизатор в Индии. Реквизиты были повторно использованы в пяти соединениях, происходящих из пяти различных IP-адресов в пределах той же подсети

провайдера в Канаде. Интересно, что выходной маршрутизатор не был доступен, когда была раскрыта попытка подслушивания. Анализ сетевого трафика, обнаруженного сервером-ловушкой, показал, что в каждой сессии было несколько посещений почтовой папки, такой как Входящие, INBOX.Sent и INBOX.Template, хотя некоторые из них (например, INBOX.Template) не были включены в качестве приманки. Это признак того, что злоумышленник, вероятно, использовал почтовый клиент, который автоматически пытается просматривать некоторые стандартные папки.

Восьмой случай произошел в первую неделю января 2011 года, и в нем участвовал узел в Германии. Пять несанкционированных соединений были произведены сервером-ловушкой из узла, находящегося в Эквадоре. Во всех случаях после успешной аутентификации на сервере, почтовый клиент злоумышленника пытался исполнить команду IMAP STARTTLS, пытаясь переключиться на соединение SSL.

Наконец, самые серьезные случаи были зафиксированы в апреле 2011 года. Два узла в ведении правительства были прослушаны. После этого были произведены попытки входа примерно в 30 различных сетях в Европе и Индии. В каждой из попыток, злоумышленник использовал стандартный клиент IMAP для доступа к счету (по аналогии с седьмым инцидентом). Инциденты произошли примерно через 16 часов после того, как были перехвачены учетные данные, и команды IMAP, выпущенные злоумышленником, оказались одинаковы в обоих случаях. Отсюда можно сделать вывод, что была использована некоторая автоматизированная программа, которая согласует выполнение попыток повторного подключения.

Один из узлов, участвующий в этом случае был замечен ранее в седьмом инциденте, но не был доступен после него. Он снова появился через несколько месяцев и теперь участвовал в скоординированной попытке с другим выходным узлом. Различные хосты использовались для попыток соединения в разное время дня. Некоторые из этих незаконных подключений даже перенаправлялись через другие маршрутизаторы Тог в попытке запутать систему. Но из-за уникального соединения между выходными узлами, удалось определить выходные узлы, использовавшиеся первоначально в качестве приманки.

Два из десяти узлов поддерживали очень высокую пропускную способность (44 и 20,8 Мбит/с соответственно). Были два узла, которые поддерживали среднюю пропускную способность около 1,4Мбит / с и 856 Кбит / с. Кроме того, было три узла, которые поддерживали низкую пропускную способность 150, 100 и 56 Кбит/с, соответственно.

Клиенты Tor стандартно создают цепи с помощью фиксированного набора узлов ввода или так называемых «сторожевых узлов» для предотвращения атаки. Оба узла высокой пропускной способности были сторожевыми узлами. Один из трех узлов низкой пропускной способности также являлся сторожевым узлом. Хотя их низкая пропускная способность дает им меньше шансов оказаться в маршруте Tor, они могут намеренно публиковать информацию о задержке, поддельную пропускную способность и время безотказной работы из-за предвзятости алгоритма выбора узлов во время создания схемы.

Интернет-трафик проходит несколько сетевых элементов, пока не достигнет своей конечной цели. Шифрованная связь используется в анонимных сетях для защиты оригинального пользовательского трафика от прослушивания в промежуточных элементах сети, таких как маршрутизаторы или точки беспроводного доступа. Тем не менее, возможность перехвата трафика не исчезает. Следовательно, передаваемые подложные сообщения в предложенном подходе могут быть подслушаны не только на выходном узле, но и на любом другом элементе сети по пути к адресату. Это означает, что в случаях, обнаруженных системой, подложные сообщения могли быть перехвачены в какой-то другой момент в маршруте между выходным узлом и сервером-ловушкой, а не на самом выходном узле.

Хотя предыдущую возможность нельзя исключать, создатели системы обнаружения считают, что во всех случаях приманка была действительно перехвачена на пораженном выходном узле по следующим причинам. Не только простота установки и эксплуатации выходных узлов, но и то, что выходные узлы поддерживаются добровольцами, не имеющими новейших программных патчей с низким уровнем безопасности, означает, что злоумышленники могут легко перехватить управление именно выходным узлом. В то же время, большинство сетевых элементов Tor находятся под контролем провайдеров или других организаций, на которых сложно перехватить учетные данные пользователя.

В будущей работе, планируется использовать несколько серверов-ловушек, разбросанных в разных сетях по всему миру, связанных с различным набором учетных данных на каждом из них. Это повысит обнаружение ситуаций, связанных с тем же выходным узлом, но разными ответами одного и того же сервера.

Анонимные сети предлагают важный сервис для пользователей, которые хотят защитить свою анонимность в Интернете. Благодаря использованию шифрования анонимные сети, такие как Tor, также защищают конфиденциальность пользовательского трафика от злоумышленников, например, в случае, когда пользователь подключен через

незащищенную публичную беспроводную сеть. Однако, поскольку эти системы не обеспечивают окончное шифрование, трафик подвергается воздействию потенциальных наблюдателей. Таким образом, для пользователей крайне важно, чтобы использовались протоколы уровня, которые поддерживают шифрование для предотвращения перехвата злоумышленником трафика на выходных узлах или между сетями.

В целях дальнейшего исследования планируется использовать больше подставных сообщений и увеличить правдоподобие и разнообразие приманок, варьировать расположение серверов-ловушек и использовать несколько копий каждого сервера в различных сетях. Также планируется расширить систему для обнаружения атак в популярных социальных сетях.

Основные выводы по результатам проведенного исследования следующие:

- общий метод для обнаружения перехвата трафика в анонимных сетях и на прокси-серверах основывается на передаче подложных реквизитов пользователя;
- прототип системы обнаружения может быть использован для имитации анонимной сети Tor. При этом обнаружено несколько случаев, когда подложные данные использовались внешним пользователем для входа на контролируемые сервера;
- метод может быть расширен для обнаружения в HTTP сессиях hijacking атак, которые могут быть использованы для перехвата активных пользовательских сессий на веб-сайтах, где не используется шифрование во время сессии.

Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 4-е изд. СПб.: Питер, 2010. 944с.
2. Chakravarty S., Portokalidis G., Polychronakis M., Keromytis A.D., Detecting Traffic Snooping in Tor Using Decoys. Available at: <http://www.cs.columbia.edu/~mikepo/papers/tordecoys.raid11.pdf>, accessed 03. 03. 2014.
3. Таненбаум Э. Компьютерные сети. 4-е изд. СПб.: Питер, 2011. 992 с.