Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.738.5

Бондарь
Кирилл Викторович

Способы ограничения анонимного доступа к интернету на предприятии

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98.80.01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Сечко Г.В.
к.т.н., доцент

_____

Библиотека БГУИР

Минск 2015

КРАТКОЕ ВВЕДЕНИЕ

Обоснование актуальности темы магистерской диссертации. Технологии защиты информации от утечек в компании постоянно развиваются и совершенствуются, но так же совершенствуются и методы кражи информации. Современные системы обнаружения и предотвращения утечек информации уязвим к использованию шифрования при передачи данных с компьютеров компании в сеть интернет. В последнее время очень активно развиваются так называемые анонимные сети, основным назначением которым было предоставления пользователям анонимного доступа к ресурсам сети интернет, т.е. исключалась возможно идентифицировать на конечном ресурсе кто именно обращается к серверу. Данную технологию активно начали использовать хакеры для осуществления взлома удаленных серверов и ухода от ответственности, т.к. в журналах атакуемого сервера значиться подставные идентификационные данные, по которым невозможно вычислить, кем была совершена атака.

Оценка современного состояния решаемой задачи. Простота использования анонимной сети породила новую угрозу для компаний в плане предотвращения утечки информации через компьютерные сети. Используя анонимную сеть, сотрудники компаний не только могут получать доступ к ресурсам, которые запрещены правилами безопасности, но и анонимно передавать данные в обход систем мониторинга, т.к. передаваемые данные находятся в зашифрованном виде и не распознаются системами контроля утечки информации.

Задачи и назначение работы. В этих условиях назначение этой работы - разработать метод анализа сетевого трафика для обнаружения использования анонимной сети в компании, а так же последующей блокировке доступа к ней.

Библиотека БГУИР

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи проводимых исследований. Согласно требования к обеспечению информационной безопасности в компании Аэромаш и недопущению утечки информации внедрены различные технические средства защиты. В связи с появлением современных угроз информационный безопасности внедренные средства защиты информации становятся уязвимыми. В этих условиях анализ этих угроз и разработка средств противодействия становится непрерывной задачей. Поэтому **целью настоящей работы** стало создание метода по анализу сетевого трафика для обнаружения использования и блокировки анонимной сети Tor чтобы изолировать канал утечки информации. Для достижения поставленной цели в этой диссертации **решены следующие задачи**:

- проведен обзор возможных средств защиты
- изучены методы перехвата и анализа сетевого трафика
- разработан метод по обнаружению и блокировке анонимной сети Tor

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики (справка о внедрении)

Личный вклад магистранта в выполненную работу. Работа полностью выполнена лично магистрантом на базе его исследований, начатых им будучи студентом предвыпускного курса БГУИР.

Результаты работы опубликованы в:

- Тезисах докл. 48-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии / под ред. В. Л. Николаенко и Г. В. Сечко, Минск: БГУИР, ИИТ, 7 – 11 мая 2012 года. – Мн.: ИИТ БГУИР, 2012.
- Материалах XVIII Междунар. науч.-техн. конф. «Современные средства связи», 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013
- Материалах II Междунар. науч.-техн. конф. «Алгоритмические и программные средства в информационных технологиях, радиоэлектронике и телекоммуникациях», 1–31 янв. 2014 года, Тольятти, Россия
- Тезисах докл. 50-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014.

Библиотека БГУИР

Результаты работы апробированы на 3 (трех) научно-технических конференциях, в том числе 1 (одной) международной:

• 49-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии / под ред. Г. В. Сечко, Минск: БГУИР, ИИТ, 4 мая 2013 года.

• XVIII Междунар. науч.-техн. конф. «Современные средства связи», 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.].

• 50-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014.

По результатам апробации на 48-й и 50-й научных конференций аспирантов и магистрантов БГУИР по направлению 8: Информационные системы и технологии первый доклад отмечен грамотой, а второй благодарностью руководства БГУИР.

Библиотека БГУИР

КРАТКОЕ СОДЕРЖАНИЕ

Работа состоит из введения, общей характеристики работы, четырёх глав и заключения.

В первой главе «Обзор предметной области» описано предприятие, системы позволяющие получить анонимность в сети интернет и принцип их работы.

В второй главе «Анализ угроз информационной безопасности» описаны современные угрозы информационной безопасности, терминология и классификация угроз и уязвимостей, проанализированы угрозы в компании Аэромаш и обозначена угроза утечки информации, с учетом существующих средств защиты.

В третьей главе «Мероприятия по парированию угроз информационной безопасности на предприятии» описаны способы предотвращения утечек информации, проведен анализ существующих средств защиты их преимущества и недостатки.

В четвертой главе «Проектирование метода для обеспечения защиты от утечки информации через анонимную сеть TOR» описана аппаратная и программная части, а также разработанные скрипты обработки, для блокировки сети TOR.

Библиотека БГУИР

ЗАКЛЮЧЕНИЕ

В результате исследования проведенного мной в рамках проекта по обеспечению информационной безопасности в компании Аэромаш, получены следующие результаты:

1. Изучены современные угрозы информационной безопасности, которые позволяют простому пользователю не имеющему специальных навыков в области компьютерных технологий и сетей, использовать программное обеспечения для анонимного доступа в сеть интернет, не требующее установки на компьютер или повышения привилегий учетной записи пользователя, а так же не обнаруживаемое программными комплексами по мониторингу приложений.

Особенностью использования анонимных сетей и ключевым моментом который позволяет обходить различные системы мониторинга и анализа содержимого сетевого трафика является многоуровневое шифрование данных которое препятствует этим системам распознать какая именно информация передается и соответственно сопоставить ее с фильтрами безопасности содержащими маркеры конфиденциальности.

Использование данной уязвимости позволяет беспрепятственно и скрытно от службы по защите информации компании Аэромаш, а так же специальных средств защиты, таких как системы обнаружения и предотвращения утечек информации, передавать конфиденциальную информацию по разработанной в компании конструкторской и технической документации по различным проектам, на разработку которых было потрачено несколько лет, во внешнюю сеть.

Этими действиями сотрудник наносит серьезный материальный ущерб интересам компании на мировом рынке, так как в большинстве случаев конфиденциальная информация которая утекла из компьютерной сети как правило попадает к конкурентам по бизнесу, экономя значительное время и финансовые ресурсы на разработку аналогов. Так же вполне реальная ситуация когда компании придется закрыть некоторые проекты результаты которых утекли к конкурентам и техническая разработка разрабатываемая многие годы становится не актуальной, тем самым теряются вложенные средства.

2. Изучены основы функционирования анонимных сетей позволяющих получить анонимность при обмене информацией в сети интернет с веб-серверами, а также файловыми хранилищами на которые можно загружать конфиденциальную информацию в обход средств обнаружения и предотвращения утечек информации.

Анонимность дает возможность скрыть от службы по защите информации компании реальный адрес сервера к которому обращается

Библиотека БГУИР

пользователь, а так же какой сервис был использован в процессе работы. Все события записываются в системные журналы но по ним нельзя установить какие действия производились.

Установлено что большинство анонимных сетей имеет клиент-серверную архитектуру с единым сервером, с которым могут устанавливать соединения клиенты и который имеет статический адрес в сети интернет. Клиент к таким сетям сложно установить на рабочую станцию пользователя не имея прав системного администратора, программа изменяет системные файлы в процессе инсталляции. Такие сети не представляют серьезной угрозы для компаний так как требуют выполнения многих условий которые по умолчанию заблокированы в компаниях с базовым уровнем информационной безопасности.

Более сложные анонимные сети такая как сеть Tor не имеет единого сервера со статическим адресом в сети интернет, ядро данной сети децентрализовано и имеет постоянно изменяющиеся адреса. Клиент для подключения к анонимной сети Tor для использования не требует специальных навыков от пользователя, так же как не требует инсталляции на рабочую станцию пользователя, соответственно не запрашивает права администратора так как не изменяет системные файлы . Основное преимущество данной сети состоит в том что при обмене информацией с сервером в сети интернет производится многоуровневое шифрование информации, а сам канал связи до конечного сервера проходит через три случайно выбранных узлов сети Tor.

Информация шифруется при передачи от рабочей станции к первому узлу сети, первый узел сети знает только адрес рабочей станции и адрес следующего узла сети, затем первый узел снова шифрует информацию и передает второму узлу сети, который не может получить какую-либо информацию об реальном отправителе, он только знает адрес первого узла сети и адрес следующего, третьего узла, информация снова шифруется и передается третьему узлу. Третий узел получив информацию дешифрует ее и отправляет на конечный сервер к которому обращается пользователь, при этом конечный сервер не сможет узнать кто является первоисточником запроса, так как видит только адрес третьего узла сети Tor. При ответе сервера на запрос алгоритм повторяется в обратном порядке и до рабочей станции пользователя доходит ответ.

Продолжительное изучение анонимной сети Tor показало ее в некотором смысле уникальность, а именно это заключается в периодически изменяемом разработчиками алгоритме, при котором также меняются уникальные маркеры пакетов по которым можно было бы обнаружить использование Tor в сети компании, данный механизм обнаружения работал два года назад. Ранее было возможным блокировать анонимную сеть на уровне системы предотвращения

Библиотека БГУИР

вторжений Cisco IPS. Также не имеет смысла блокировать какой либо конкретный узе сети, так как при недоступности одного входного узла клиент пытается подключиться к следующему из списка. Список распространяется клиенту по внутреннему протоколу и получить его невозможно.

Постоянная модификация программного обеспечения поддержки анонимной сети с целью исключить возможность обнаружения, блокировки использования или деанонимизацией клиентов существенно усложняет задачу по обеспечению информационной безопасности специалистам по защите информации, что привело к необходимости исследовать угрозу и разработать метод по ее парированию описанный в данной магистерской диссертации.

3. В результате исследования угроз со стороны анонимной сети Tor был разработан метод по их парированию. Цель метода в формировании списка IP адресов всех узлов анонимной сети Tor. Метод заключается в перехвате и анализе специально разработанными алгоритмами сетевого трафика передаваемого от собственного веб-сервера в интернете через цепочку анонимной сети Tor, в ответ на запрос от рабочей станции. Пакеты специально формируются сервером с нестандартным размером что никак не влияет на производительность и принимаются системой без ошибок, этот размер мы берем в качестве маркера. Пакет отправляется в ответ на запрос от рабочей станции находящейся на территории компании Аэромаш с установленным на ней клиентом анонимной сети Tor. Весь интернет трафик компании зеркалируется на специальный сервер который использует разработанный алгоритм для анализа и выделение маркера переданного в пакете от веб-сервера в интернете.

Когда пакет с маркером найден, алгоритм определяет IP адрес источника и добавляет его в файл, после чего содержимое файла синхронизируется со списком IP адресов узлов сети Tor находящемся на собственном веб-сервере по адресу http://trustsecurity.by/list7829.txt, алгоритм синхронизации введен в связи с нестабильным соединением с сетью интернет. На основе IP адресов собранных в файле производится их блокировка на межсетевом экране компании, но как описано выше Tor может обратиться к другому узлу сети, в этом случае IP адрес нового узла также будет определен и заблокирован.

Таким образом в течение суток файл заполняется IP адресами всех узлов сети Tor. В случае появления новых узлов они так же попадают в список блокируемых.

В результате в сети компании становится невозможно использовать анонимную сеть Tor и соответственно утечка информации становится невозможной.

Побочным результатом исследования стало использования списка адресов узлов анонимной сети Tor для фильтрации на серверах компании в

Библиотека БГУИР

интернете. Количество сетевых атак значительно сократилось. Если ранее приходилось по одному выявлять адреса атакующих машин и блокировать их, что требовало некоторого времени, то теперь 80 процентов этих адресов заблокированы, так как большинство атак производилось с использование анонимной сети Tor.

На моем сайте по адресу http://trustsecurity.by/list7829.txt бесплатно доступен список адресов недельной давности, а актуальный с постоянными обновлениями для подписчикам которые хотят защитить свои веб сервера и сеть компании предоставляется за определенную плату.

Библиотека БГУИР

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Бондарь К.В.Защита корпоративной ит инфраструктуры от использования анонимной сети TOR // 49-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез.докл. (Минск, 4 мая 2013 года). – Мн.: БГУИР, 2013. – 68 с. с ил. – С. 68-69

2-А. Бондарь К.В.Блокировка анонимного доступа в интернет для корпоративной сети // Современные средства связи: материалы XVIIIМеждунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 299 с. – С. 253-254.

3-А. Бондарь К.В. Методы защиты от использования анонимной сети TOR // Алгоритмические и программные средства в информационных технологиях, радиоэлектронике и телекоммуникациях: материалы IМеждунар. заочн. науч.-техн. конф., 1–31 янв. 2014 года, Тольятти, Россия / – Тольятти: ПГУС, 2014. – 114 с. – С. 89-90.

4-А. Бондарь К.В. Механизм выявления использования анонимного доступа в интернет через сеть TOP из корпоративной сети компании и блокировки такого доступа // 50-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез.докл. (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014. – 78 с. с ил. – С. 7.

Библиотека БГУИР