Д. А. Мельников, В. Р. Петров, А. Н. Радько, Д. С. Бурый, С. А. Хрусталев

ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИХ СИСТЕМ НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА[1]

Введение

Указ Президента Российской Федерации от 15 января 2013 г. №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» определил следующие основные задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации [1].

Ежегодно наблюдается постоянный рост киберпреступлений в Интернете [2, 3]. Только в 2012 г. ущерб от киберпреступности был оценен в $2 миллиарда в год в России и в $110 миллиардов во всем мире! Цифры говорят сами за себя. При этом выявление самих киберпреступников остается весьма сложной задачей, решение которой в большинстве случаев найти невозможно. В частности, растет число каналов утечки информации, что в условиях массового использования радиотехнических средств информационного обмена (включая системы мобильной (сотовой) связи) является серьезной угрозой как для государственной безопасности, так и для корпоративной.

Противодействие компьютерному шпионажу

Современные методы и способы противодействия компьютерному шпионажу фактически основаны на контроле и анализе глобального сетевого трафика [3, 4, 5], так как весьма сложно, а порой и практически невозможно предугадать (спрогнозировать) направления передачи вредоносного трафика. При этом важно не только обнаружить вредоносный трафик, но и установить авторство (принадлежность) такого трафика, особенно в условиях активного и широкомасштабного использования способа проведения атак типа «маскарад».

С другой стороны, анализ трафика является неотъемлемой процедурой сетевых программно-аппаратных комплексов (ПАК), включая ПАК для управления сетью и потоками данных (коммутаторы, маршрутизаторы, трансляторы сетевых адресов и т. п.) и ПАК обеспечения информационной безопасности (ИБ) (сетевые экраны, сенсоры, криптомаршрутизаторы и т. п.).

Таким образом, анализ трафика является весьма эффективной, а в некоторых случаях и единственной контрмерой по противодействию сетевым атакам и каналам утечки информации, которая предусматривает проведение определенных мероприятий по контролю защищенности

[1] Данная работа выполнена в НИЯУ МИФИ и МГУЭСИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполняемого совместно с ООО «ОКБ САПР» по договору № 02.G25.31.0050.

информационно-технологической инфраструктуры Российской Федерации и, самое главное, установлению причин произошедших и прогнозируемых компьютерных инцидентов.

Анализ сетевого трафика — это совокупность информационно-технологических и инженерно-технических мер по приему и обработке сетевого трафика. Очевидно, что анализ трафика может использоваться для борьбы с угрозами ИБ, а может — и в противоправных целях. Поэтому в данной статье и применяется термин «контрмера», что предусматривает использование методов и способов обеспечения ИБ, которые фактически применяют киберпреступники для проведения своих атак, но только в противоправных целях. Если преступник использует анализ трафика для получения разного рода информации для последующего проведения атак типа «маскарад», то специалисты в области ИБ используют анализ сетевого трафика для парирования угроз ИБ.

В правовом аспекте в настоящее время разрабатываются новые законопроекты, предусматривающие ужесточение наказания за компьютерные атаки. В частности, в статью 272 Уголовного кодекса РФ («Неправомерный доступ к компьютерной информации») предложено внести целую новую часть (пятую), которая предусматривает ответственность за преступления, если они «повлекли ущерб безопасности критической информационной инфраструктуры Российской Федерации или создали угрозу его наступления» [6]. Наказание — лишение свободы на срок до десяти лет (сегодня самое суровое наказание — до семи лет).

Программная реализация и практическое использование анализатора трафика

Для решения задачи анализа сетевого трафика был разработан пакет прикладных программ (ПО) для приема сетевых пакетов и их визуальной обработки (программный анализатор трафика — ПАТ). ПО разработано для ОС *Linux* (*Ubuntu*) и написано на языке программирования *Python*, с использованием прикладного программного интерфейса *Linux API* и графической библиотеки *Tkinter*. Для последующей работы с полученной информацией был реализован вывод в текстовый файл. Запуск программы осуществляется как с помощью терминала, так и с помощью графического модуля (в том случае, если будут получены права администратора в графическом интерфейсе).

Анализаторы трафика широко используются системными администраторами ИБ для обнаружения проблем ИБ и «узких мест» сети. Анализ трафика может проводиться в различных компонентах сети, а именно:

- ПАТ встраивается в маршрутизатор (шлюз). В данном случае можно контролировать трафик, проходящий через интерфейсы данного шлюза. В частности, интернет-провайдер способен контролировать вредоносный трафик, поступающий на компьютеры его пользователей, а также передаваемый последними в сеть;
- ПАТ встраивается в оконечный узел сети. Используя ПАТ Ethernet-сети, можно контролировать трафик двумя способами. «Классический»: некоммутируемая Ethernet-сеть предполагает, что каждый сетевой адаптер просматривает весь трафик своего Ethernet-сегмента; в данном режиме можно контролировать только «собственный трафик». Для контроля трафика всего Ethernet-сегмента требуется перевести сетевой адаптер в режим прослушивания, чтобы ПАТ мог анализировать все поступающие на сетевой адаптер пакеты, включая и те, которые ему не предназначены.

Как правило, анализаторы трафика общего использования различаются между собой в основном только функциональными возможностями и предназначены для анализа собственного трафика.

Первые результаты тестирования

Разработанный ПАТ тестировался в реальной Ethernet-сети (локальной вычислительной сети). На этом этапе испытаний осуществлялся прием байтовых последовательностей, разделенных на сетевые пакеты. Каждый пакет отображался на экране компьютера в шестнадцатеричном формате, пригодном для визуального анализа (рис. 1).

```
Got a 78 byte packet

0000   45 00 00 4E 43 29 00 00    E..NC)..
0008   80 11 73 11 C0 A8 01 15    ..s.....
0010   C0 A8 01 FF 00 89 00 89    ........
0018   00 3A 0E AD F8 DF 01 10    .:......
0020   00 01 00 00 00 00 00 00    ........
0028   20 45 45 45 46 45 4F 43     EEEFEOC
0030   4E 49 50 49 4B 43 41 43    NIPIKCAC
0038   41 43 41 43 41 43 41 43    ACACACAC
0040   41 43 41 43 41 43 41 41    ACACACAA
0048   41 00 00 20 00 01          A.. ..
```

Рис. 1. Отображение принятого пакета на экране компьютера

В некоторых случаях для получения необходимой информации и более точного анализа принятого пакета требуется выделение всех заголовков пакета, относящихся к различным уровням интернет-архитектуры (пятиуровневая модель взаимодействия открытых систем) [4, 5]. При такой детализации полученная информация может иметь вид:

ETHER: Destination address: 0000BA5EBA11
ETHER: Source address: 00A0C9B05EBD
ETHER: Frame Length: 1514 (0x05EA)
ETHER: Ethernet Type: 0x0800 (IP)
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Service Type = 0 (0x0)
IP: Precedence = Routine
...

На следующем этапе тестировался экранный интерфейс разработанного ПАТ. Для запуска программы используется системное приложение «Терминал», представленное на рис. 2.

Рис. 2. Запуск программы

Далее открывается директория, где находится ПАТ. Для изменения режима доступа к файлу используется команда «chmod». Активирование ПАТ представлено на рис. 3.

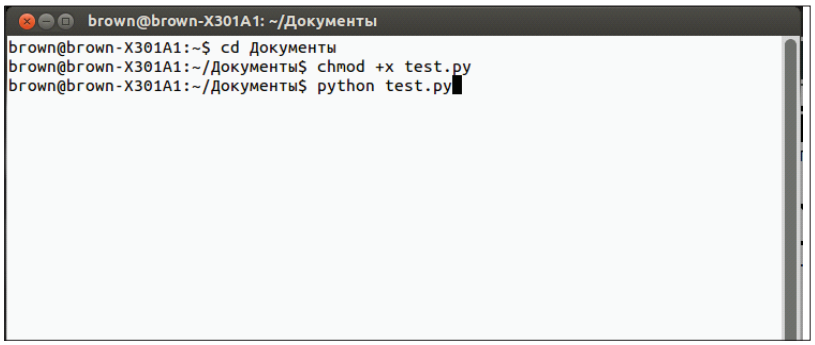

Рис. 3. Активирование ПАТ

С начала функционирования ПАТ принял и отобразил на экране несколько сетевых пакетов (рис. 4).

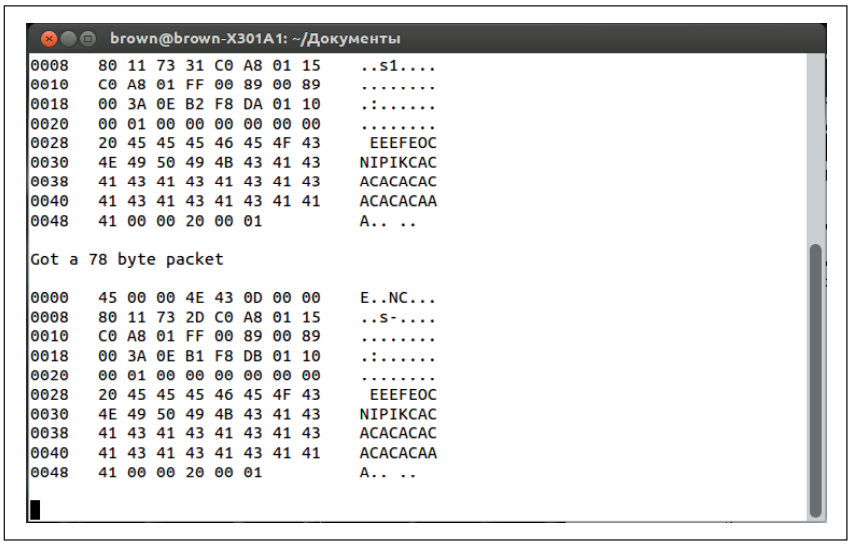

Рис. 4. Принятые и отображенные ПАТ пакеты

Обнаружение скрытого порта

В процессе дальнейшего тестирования и проверки работоспособности ПАТ в условиях домашней ЛВС, развернутой на базе концентратора ASUS (4 интерфейса RJ-45 и интерфейс WiFi), были обнаружены входящие и исходящие сетевые пакеты проигрывателя мультимедиа «Apple TV» (рис. 5). При этом следует отметить, что информационный обмен через интерфейс WiFi между проигрывателем мультимедиа «Apple TV» и концентратором ASUS продолжался и при выключенных телевизоре и проигрывателе (оба не отключались от сети электропитания)!

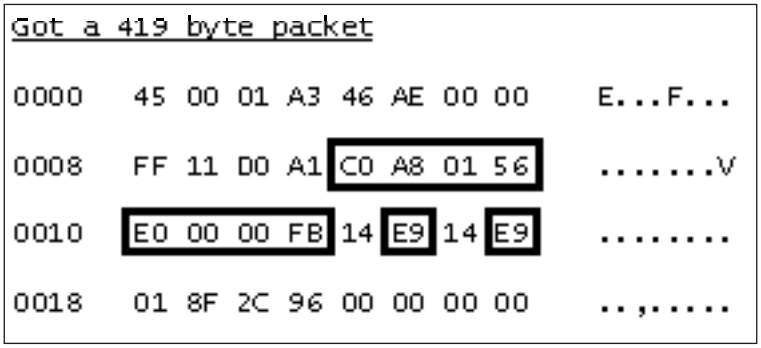

Рис. 5. Принятый пакет, который был получен в период информационного обмена между проигрывателем мультимедиа «Apple TV» и концентратором ASUS

В процессе визуального анализа и декодирования были получены следующие данные (рис. 5):

- Отправитель: 192.168.1.134, UDP-порт 233;
- Получатель: 224.0.0.251, UDP-порт 233.

В стандарте RFC-1700 [7] представлена информация о том, что 233-й порт является зарезервированным (рис. 6). Поэтому возникает проблема неоднозначности относительно принадлежности указанного порта транспортного уровня. Очевидно, что компания Apple осуществляет поиск и мониторинг произведенных ею сетевых ПАК. Тем не менее конечные цели

такого поиска и мониторинга не известны, но не исключено, что это вполне может быть один из скрытых каналов управления, предназначенных для «негласного съема» информации[2] [4, 5]. Фактически перед нами возможный пример компьютерного шпионажа!

```
cdc             223/tcp    Certificate Distribution Center
cdc             223/udp    Certificate Distribution Center
#               Kannan Alagappan <kannan@sejour.enet.dec.com>
#               224-241    Reserved
#                          Jon Postel <postel@isi.edu>
#               242/tcp    Unassigned
```

Рис. 6. Выписка из стандарта RFC-1700

Выводы

В данной статье рассмотрена процедура анализа трафика, которая является весьма эффективной, а в некоторых случаях и единственной контрмерой по противодействию сетевым атакам и каналам утечки информации и предусматривает проведение определенных мероприятий по контролю защищенности информационно-технологической инфраструктуры Российской Федерации и, самое главное, установлению причин произошедших и прогнозируемых компьютерных инцидентов.

Также в статье рассмотрен разработанный ПАТ, который сразу же позволил выявить скрытый канал управления, предназначенный для «негласного съема» информации. В связи с этим работа над ПАТ будет продолжена, что предусматривает разработку программного учебно-методического комплекса для проведения лабораторных и исследовательских работ для выявления и предотвращения компьютерных атак и ликвидации каналов утечки информации (скрытых каналов управления).

СПИСОК ЛИТЕРАТУРЫ:

1. Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».
2. Интернет-ресурс www.startupafisha.ru/news/itogi-issledovaniya-kiberprestupnost-v-rossii-i-mi/$.
3. *McNamara J.* Secrets of Computer Espionage: Tactics and Countermeasures. New York: John Wiley & Sons, Inc., 2003.
4. *Мельников Д. А.* Организация и обеспечение безопасности информационно-технологических сетей и систем: Учебник. М.: IDO Press, Университетская книга, 2012.
5. *Мельников Д. А.* Информационная безопасность открытых систем: Учебник. М.: ФЛИНТА, Наука, 2013.
6. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Статья 272 «Неправомерный доступ к компьютерной информации».
7. *Reynolds J., Postel J.* Assigned Numbers. RFC 1700. October 1994.

[2] По информации, «просочившейся» в Интернет, одна из последних версий ОС «MAC OS» разрабатывалась компанией Apple совместно с Агентством национальной безопасности США.