ных колонок в отдельный список. После этого датасет разделен на две части – первая часть предназначалась для обучения нейронной сети, вторая же часть для апробации.

Применив стандартную модель классификации, был получен результат корректности предсказания оттока клиентов банка, равный 64,52%. За счет применения разработанного алгоритма подбора гиперпараметров, а именно использования метода кросс-валидации и стратификации со случайным распределением был получен результат корректности предсказания оттока клиентов банка, равный 74%. Таким образом, модель на базе предложенного подхода решения задачи прогнозирования оттока клиентов, основанная на использовании нейронной сети с предварительным определением гиперпараметров, показала лучший результат, чем классический вариант решения подобных задач, применяемый на практике.

ЛИТЕРАТУРА

1. Электронный ресурс, http://www.consultant.ru/document/cons_doc_LAW_154161/, Распоряжение Правительства РФ от 01.11.2013 N 2036-р (ред. от 18.10.2018) “Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года”.

2. Электронный ресурс, https://www.calltouch.ru/glossary/churn-rate, “Churn rate”.

3. Электронный ресурс, https://vc.ru/marketing/156703-12-sposobov-nemedlenno-ostanovit-ottok-klientov, “12 способов немедленно остановить отток клиентов”.

УДК 003.26

Я. Ласык[1], ассист.; Д.М. Романенко[2], доц., канд. техн. наук
П.П. Урбанович[2], проф., д-р техн. наук
[1](Люблинский Католический университет, Польша), [2](БГТУ, г. Минск)

ИСПОЛЬЗОВАНИЕ СЕТЕВЫХ ПРОТОКОЛОВ И СТЕГАНОГРАФИИ ДЛЯ ТАЙНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

В последнее время наблюдается новый и опасный тренд: все больше разработчиков вредоносного ПО и средств кибершпионажа прибегают к использованию стеганографии.

Современные методы компьютерной стеганографии условно можно поделить на 2 класса:

1) методы сокрытия информации в контенте, а также в альтернативных потоках данных (Alternate Data Streams, ADS) файловой си-

стемы NTFS;

2) методы сокрытия информации в структуре сетевых протоколов.

Сетевое взаимодействие является ключевым элементом функционирования любой вредоносной программы, а также тайно передаваемой информации [1–2].

Этому способствуют три главные причины, связанные со стеганографией [3]:

1) стеганография позволяет скрыть сам факт загрузки/выгрузки данных, а не только сами данные;

2) стеганография помогает обойти DPI-системы, что актуально в корпоративных сетях; система DPI (Deep Packet Inspection – глубокая проверка пакетов), как видно из названия, выполняет глубокий анализ всех проходящих через нее пакетов. Термин «глубокий» подразумевает анализ пакета на верхних уровнях модели OSI, а не только по стандартным номерам портов. Помимо изучения пакетов по стандартным паттернам, по которым можно однозначно определить принадлежность пакета определенному приложению (по формату заголовков, номерам портов и т. п.), система DPI осуществляет и так называемый поведенческий анализ трафика, который позволяет распознать приложения, не использующие для обмена данными заранее известные заголовки и структуры данных. популярными становятся интегрированные в маршрутизаторы решения DPI;

3) использование стеганографии может позволить обойти проверку в AntiAPT-продуктах, поскольку последние не могут обрабатывать все графические файлы (их слишком много в корпоративных сетях, а алгоритмы анализа довольно дорогие).

Тайная и трудно обнаруживаемая (как факт) передача информации, основанная на стеганографическом преобразовании (модуляции) элементов и структур сетевых протоколов все чаще применяется там, где появляются запреты или ограничения на легальное использование Интернета.

Скрытые каналы в протоколах компьютерных сетей аналогичны методам сокрытия информации в звуковом, визуальном или текстовом контенте. В то время как классическая стеганография требует какой-либо формы контента в качестве прикрытия, скрытые каналы требуют некоторого сетевого протокола в качестве носителя скрытой информации, передаваемой от одного абонента к другому.

Можно определить различные модели скрытого сетевого взаимодействия двух абонентов (*A* и *B*) в зависимости от того, являются ли *A* и *B* отправителем и получателем открытого канала (Overt Sender

и Overt Receiver) или же они действуют как посредники (*C*) и манипулируют открытым каналом между ничего не подозревающими пользователями. Рассмотрим особенности такого взаимодействия, основываясь на известной модели Симмонса [4].

Если отправитель (*A*) скрытого канала также является отправителем открытого канала, он может манипулировать открытым каналом по желанию (например, чтобы максимизировать пропускную способность скрытого канала или его скрытность). Однако иногда скрытый отправитель может быть не в состоянии создать открытый канал или может не делать этого для большей скрытности. В этом случае отправитель может выступать в качестве посредника, встраивая скрытый канал в существующий открытый канал. Очевидно, что тогда скрытый отправитель не имеет контроля над открытым каналом, и максимальная пропускная способность скрытого канала зависит от существующего открытого канала.

Скрытый получатель (*B*) может быть получателем открытого канала, но для повышения скрытности получатель также может быть посредником (*C*), извлекающим скрытую информацию из открытого сообщения, предназначенного для невиновного получателя. Затем скрытый приемник должен (если возможно) удалить скрытый канал, предотвращая возможное обнаружение приемником или любыми другими промежуточными узлами.

На рис. 1 показаны возможные комбинации скрытых местоположений отправителя и получателя. Фактический сценарий связи зависит от применения скрытого канала.

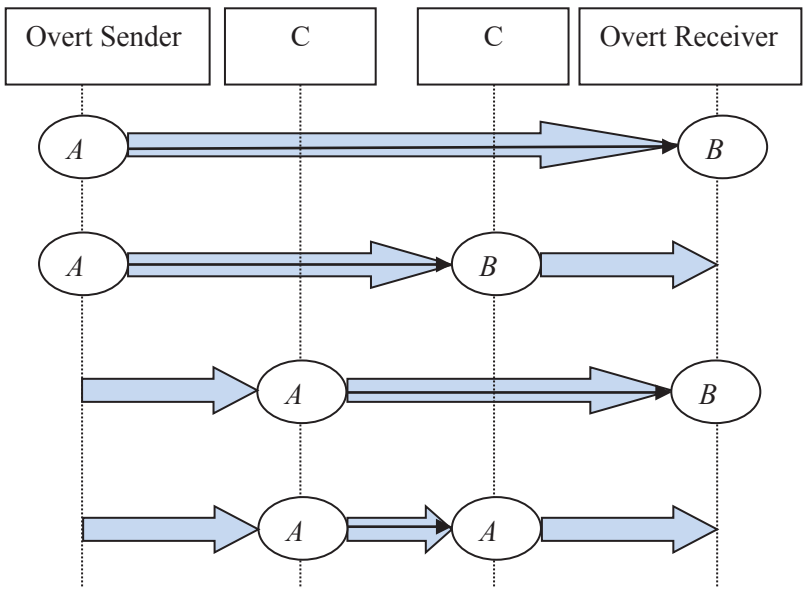

Рисунок 1 – Модели взаимодействия абонентов на основе скрытых сетевых каналов

Если скрытый канал используется для обхода цензуры, скрытые и явные отправитель/получатель, вероятно, будут идентичными. Если же канал используется хакером для внешней фильтрации данных, скрытые отправитель и получатель, вероятно, будут посредниками (например, отправитель может находиться внутри стека сетевых протоколов скомпрометированной машины, а получатель может находиться на маршрутизаторе, близком к краю скомпрометированной сети).

Традиционно (см., например, [3, 5]) скрытые каналы подразделяются (хотя принципиального различия между ними нет) на

1) каналы памяти (скрытые каналы памяти) и

2) каналы временнЫе (скрытые каналы времени).

Каналы памяти (Storage Channel) предполагают прямую/косвенную запись значения объекта (осаждение тайной информации) отправителем и прямое/косвенное считывание значений объекта (извлечение тайной информации) получателем. Обычно имеется в виду, что у процессов с разными уровнями безопасности имеется доступ к некоторому ресурсу (например, к некоторым секторам диска).

Скрытые каналы рассматриваемого типа могут быть закодированы в неиспользуемых или зарезервированных битах заголовков кадров или пакетов. Это особенно проблематично, если стандарты протоколов не требуют конкретных значений или получатели не проверяют стандартные значения. На этой основе могут создаваться следующие типы скрытых каналов:

• неиспользуемые биты поля *Типа обслуживания* (Type of Service, ToS);

• *Заголовок IP*;

• поля *Флагов заголовка* TCP;

• бит *Don't Fragment* (DF) заголовка IP; биту DF можно присвоить произвольное значение, если отправителю известен размер Максимальной единицы передачи (Maximum Transfer Unit, MTU) пути к получателю, и он отправляет только пакеты размером меньше MTU;

• поле *Указателя важности* (TCP Urgent Pointer, применяется для указания данных с высоким приоритетом) – 16-битное поле, которое принимается во внимание только для пакетов с установленным флагом URG;

• сегмент *Флага сброса соединения* (TCP Reset – сегменты TCP с установленным флагом RST обрывают соединение и обычно не содержат данных) и др.

Временные каналы (Timing Channels) включают сигнальную

информацию отправителя, модулируя (осаждая тайную информацию) использование ресурсов (например, использование ЦП) с течением времени таким образом, чтобы получатель мог наблюдать за этим и декодировать (извлекать) информацию. К наиболее известным методам создания таких каналов можно отнести использование поля *Время жизни* (Time-to-Live, TTL). В IPv4 TTL представляет собой восьмиразрядное поле IP-заголовка, которое определяет максимальное количество *хопов* (hop – прыжок, участок между маршрутизаторами), которые пакет может пройти. Наличие этого параметра не позволяет пакету бесконечно ходить по сети. Каждый маршрутизатор при маршрутизации должен уменьшать значение TTL на единицу, но некоторые шлюзы можно настроить, чтобы игнорировать это. Пакеты, не достигшие адресата, но *время жизни* которых стало равно нулю, уничтожаются, а отправителю посылается сообщение *ICMP Time Exceeded*. Если требуется, чтобы пакет не был маршрутизирован, т. е. был принят только в своем сегменте, то выставляется TTL=1. На отправке пакетов с разным временем жизни основана трассировка их пути прохождения (Traceroute). Максимальное значение TTL=255. Обычное начальное значение TTL=64 (Linux, Mac, Android, iOS), TTL=128 (Windows).

Проанализированные подходы предполагают использование только одного сетевого протокола из стека TCP/IP для создания тайного канала. Модификация протокола может быть применена либо к PDU (Protocol Data Unit), либо к временнЫм отношениям между обмениваемыми PDU, либо одновременно к обоим из указанных параметров. Этот вид сетевой стеганографии можно назвать внутрипротокольной стеганографией.

Задача обнаружения скрытых каналов на основе сетевой стеганографии состоит в том, чтобы найти потенциальные скрытые каналы, которые могут быть реализованы в сети. Второй шаг – анализ выявленных каналов для оценки уровня угрозы каждого из них.

Скрытые каналы могут создаваться и использоваться не только злоумышленниками. Эти каналы могут использоваться для передачи данных аутентификации. Сетевые администраторы могут использовать скрытые каналы для защиты связи, управления сетью, скрывая эту информацию от хакеров.

ЛИТЕРАТУРА

1. Урбанович, П.П. Киберпространство: тренды, угрозы и безопасность / П.П. Урбанович // Интеграция и развитие научно-технического и образовательного сотрудничества – взгляд в будущее:

сборник статей II Междунар. научно-техн. конф. "Минские научные чтения – 2019", Минск, 11-12 декабря 2019 г.: в 3 т. Т. 3. – Минск: БГТУ, 2020. – С. 180–185.

2. Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. – Lublin : Wydawnictwo KUL, 2004. – 150 p.

3. Zander, S. Covert channels and countermeasures in computer network protocols / S. Zander, G. Armitage, P. Branch // IEEE Communications Surveys & Tutorials. – 2007. – № 9(3). – P. 44-56.

4. Simmons, G.J. The Prisoners' Problem and the Subliminal Channel / G. J. Simmons. – Proc. Advances in Cryptology (CRYPTO). – 1983. – P. 51–67.

5. National Computer Security Center, US DoD, Trusted Computer System Evaluation Criteria, Tech. Rep. DOD 5200.28- STD, National Computer Security Center, Dec., 1985.

УДК 004.056

О.Л. Сапун, доц., канд. пед. наук; А.С. Гончар, маг.
(БГАТУ, г. Минск)

ПРИМЕНЕНИЕ МЕЖСЕТЕВОГО ЭКРАНА ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Большинство предприятий сталкиваются с проблемами в компьютерных системах и утечки важной информации. Не являются исключением и предприятия агропромышленного комплекса. Существует множество программ или программно-аппаратных систем, позволяющих минимизировать данные проблемы.

Межсетевой экран (firewall, МЭ) – программная или программно-аппаратная система, обладающая искусственным интеллектом, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивающая защиту информационной системы посредством фильтрации информации [1].

МЭ выступает сегодня как наиболее действенное средство управления безопасностью. При многократно возросшем трафике данных очень важно, чтобы никакой вредоносный объект не проник в сеть организации. Проверки данных нужно проводить регулярно для поддержания системы, также необходимо проводить регулярно проверки антивирусами для обеспечения защиты операционной системы на виртуальном сервере и мониторинг безопасности сети.