DOI 10.37882/2223-2966.2023.8-2.23

ОБНАРУЖЕНИЕ И ИСКЛЮЧЕНИЕ ОБФУСЦИРОВАННЫХ КАНАЛОВ УТЕЧКИ ДАННЫХ В КОРПОРАТИВНЫХ СЕТЯХ

DETECTION AND PREVENTION OF OBFUSCATED DATA LEAK CHANNELS IN CORPORATE NETWORKS

A. Mansurov
A. Lependin
D. Ruder
P. Ladygin

Summary. This paper discusses the important problem of detection and prevention of hidden obfuscated data leak channels inside the protected areas of corporate networks. Typically, these channels are initiated by the malicious software components executed at the users' workstations. Simulation, consecutive study of their operating principles, and methods of masquerading the confidential data transfer as the regular HTTP and DNS network traffic are conducted in details. Following the results of the study, several effective approaches are proposed to identify and eliminate the operation of such hidden data leak channels inside the protected areas of corporate networks.

Keywords: network security, traffic obfuscation, data leak channels, traffic filtering.

Мансуров Александр Валерьевич
Канд. техн. наук, доцент,
Алтайский государственный университет, г. Барнаул,
mansurov.alex@gmail.com
Лепендин Андрей Александрович
Канд. физ-мат. наук, доцент,
Алтайский государственный университет, г. Барнаул,
andrey.lependin@gmail.com
Рудер Давыд Давыдович
Канд. физ-мат. наук, доцент,
Алтайский государственный университет», г. Барнаул,
ddruder@gmail.com
Ладыгин Павел Сергеевич
Старший преподаватель,
Алтайский государственный университет, г. Барнаул,
pavel-ladygin@yandex.ru

Аннотация. В работе обсуждается важная проблема идентификации и устранения скрытых каналов утечки конфиденциальной информации за пределы защищенного сегмента корпоративной сети, инициируемых вредоносным программным обеспечением на рабочих станциях пользователей. Выполнено моделирование и исследованием работы такого скрытого канала, использующего маскировку под регулярный обмен данными с использованием двух распространенных сетевых протоколов прикладного уровня — HTTP и DNS. На основании проведенного моделирования и исследования принципов маскировки передаваемых данных сформирован ряд мер, необходимых для обнаружения и предотвращения работоспособности таких скрытых каналов внутри защищенного сегмента корпоративной сети.

Ключевые слова: сетевая безопасность, обфускация трафика, утечка данных, фильтрация трафика.

Введение

Вопрос контроля сетевого трафика на границе корпоративной сети является одним из важных моментов в процессе обеспечения защищенной работы корпоративной сети и защиты информационных систем любого современного предприятия. Анализ и выявление подозрительных попыток установить соединения к критичным сервисам корпоративной сети извне или подозрительные соединения и обмен данными из корпоративной сети во внешний мир должны вовремя распознаваться и блокироваться. Для этого, как правило, применяются современные многофункциональные прокси-серверы, межсетевые экраны следующего поколения, системы обнаружения и предотвращения вторжений и системы глубокого анализа трафика (DPI — Deep Packet Inspection) [1].

Сложность обнаружения таких скрытых каналов обмена информацией, которые организованы нарушителем (злоумышленником) многократно повышается, если нарушитель маскирует свой обмен под протоколы обмена данными популярных и часто используемых корпоративных решений для организации удаленной и совместной работы, телеконференций и систем телефонии [2,3]. Такие известные решения, как SkypeMorph [4], StegoTorus [5], CensorSpoofer [6] ориентируются на тот факт, что применяемые в корпоративной сети и на ее периметре средства контроля, обнаружения, анализа и предупреждения будут воспринимать организованный ими обмен как нормальный «штатный» обмен соответствующих корпоративных приложений и не идентифицируют его как опасный, который необходимо заблокировать.

Отдельную сложность представляет задача обнаружения скрытого обмена с использованием широко востребованных в корпоративных решениях протоколов прикладного уровня, таких как протоколы HTTP, HTTPS, DNS, NTP, RDP и т.п., а также протокола ICMP [7,8]. В этом случае штатные средства и системы, обеспечивающие

работу корпоративной сети, выступают посредниками для организованных DNS- и ICMP-туннелей, а также используют предусмотренные администраторами сети возможные «открытые» пути для пропуска таких протоколов на границе. Обнаружение таких каналов скрытого обмена требует более тщательного анализа и мониторинга трафика указанных протоколов с применением методик статистического и поведенческого анализа, что удорожает и усложняет процесс.

В данной работе выполняется моделирование и исследование принципов работы возможного скрытого канала утечки конфиденциальной информации из защищенного сегмента корпоративной сети путем маскировки под обмен популярных протоколов прикладного уровня. По результатам моделирования и исследования формируются меры и подходы по обнаружению и противодействию возникновения и работы таких скрытых каналов утечки данных.

Моделирование и исследование работы потенциального канала скрытого информационного обмена

Потенциальный скрытый канал утечки конфиденциальной информации из защищенного сегмента корпоративной сети функционирует с использованием двух востребованных прикладных протоколов — протокола HTTP (или HTTPS) и протокола DNS. Согласно модельной концепции, протокол HTTP используется как основной канал передачи конфиденциальной информации за пределы сегмента корпоративной сети, а протокол DNS обеспечивает канал синхронизации отправляемой информации для обеспечения корректного получения передаваемых данных на стороне нарушителя. Выбор двух этих протоколов неслучаен. Во-первых, это одни из самых популярных протоколов сетевого взаимодействия, активно применяемых в работе корпоративных решений и элементов распределенных информационных систем (которые в настоящее время все больше становятся веб-ориентированными). В достаточно большом случае ряд компонентов (серверная составляющая, например, для клиент-серверных решений) таких распределенных систем находится за пределами сегмента корпоративной сети (в сети Интернет как облачная компонента, например). Во-вторых, для этих протоколов в корпоративной сети практически всегда есть штатные «посредники» — прокси-серверы или иные серверы, которые эффективно могут быть использованы для маскировки исходной точки происхождения трафика и дальнейшего введения в заблуждение систем пограничного контроля и анализа трафика. Концептуальная схема работы скрытого канала утечки конфиденциальной информации с использованием двух протоколов прикладного уровня приведена на рис. 1.

Вредоносное программное обеспечение (ПО), внедренное нарушителем на рабочую станцию в корпоративной сети, осуществляет отправку конфиденциальной информации на рабочую станцию нарушителя за пределами корпоративной сети с помощью протокола HTTP или HTTPS. Происходит имитация штатной работы «запрос-ответ» некоторого приложения-браузера (вредоносное ПО) с некоторым веб-сервером (ПО на рабочей станции нарушителя) в определенном домене (который контролирует нарушитель), в роли которого выступает рабочая станция нарушителя. При этом применяются штатные настройки рабочей станции для работы с данными протоколами, требующие использования корпоративного прокси-сервера (чаще всего это именно так). Корпора-

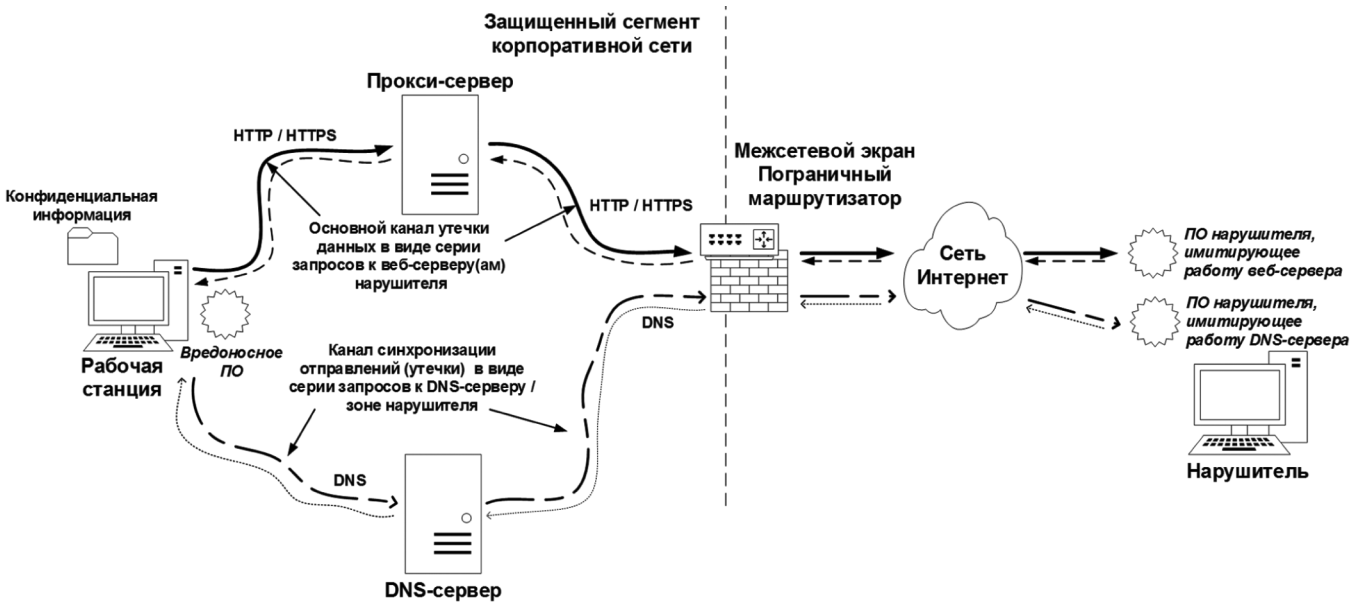

Рис. 1. Концептуальная схема работы скрытого канала утечки конфиденциальной информации

тивный HTTP/HTTPS прокси-сервер является эффективной точкой контроля и анализа веб-трафика с использованием как встроенного в функционал прокси-сервера средств проверки, ограничения и блокирования, так и с привлечением дополнительных «пристыковывающихся» решений, таких как средства антивирусной защиты, анализа передаваемых данных и интеграции в единое пространство безопасности корпоративной сети (домен безопасности Active Directory и т.п.). Весь веб-трафик во внешний мир отправляется от адреса сетевого интерфейса прокси-сервера. Это позволяет скрыть истинного инициатора сетевого взаимодействия (рабочие станции и приложения на них), а также предусмотреть «облегченный» вариант контроля и ограничений средствами на границе сети, считая трафик от прокси-сервера во внешний мир уже прошедшим необходимые проверки и фильтрацию своими силами.

Дополнительный канал, необходимый для синхронизации отправляемых фрагментов и их упорядочивания после получения на стороне нарушителя, обеспечивается при помощи протокола DNS. Здесь вредоносное ПО имитирует DNS-запросы с целью получения информации о хостах, находящихся в определенном домене (DNS-зоне), который полностью контролирует нарушитель. Поскольку в корпоративной сети функционирует штатный корпоративный DNS-сервер, то он эффективно выступает в роли посредника, ретранслируя все запросы во внешний мир от своего адреса. Все ретранслируемые запросы попадают на рабочую станцию нарушителя, где они обрабатываются ПО, имитирующим работу DNS-сервера, контролирующего ранее обозначенный домен (DNS-зону). Использование протокола DNS для организации чистого DNS-туннеля [7] может вызвать подозрения при обнаружении в ходе анализа трафика большого количества DNS-запросов больших размеров, в то время как серия типичных DNS-запросов может быть легко проигнорирована как случай штатной работы DNS-серверов.

На рабочей станции нарушителя комплексно работает ПО, которое имитирует работу веб-сервера, получающего запросы от корпоративного прокси-сервера, и имитирует работу DNS-сервера, получающего запросы от корпоративного DNS-сервера (или иного в рамках иерархии DNS-серверов). На каждый запрос формируется штатный ответ сообразно поступившему запросу для дальнейшего введения в заблуждение действующих систем анализа сетевого трафика на границе корпоративной сети и самих корпоративных DNS- и прокси-серверов путем маскировки под правильный и ожидаемый обмен данными в рамках режима «запрос-ответ».

Детальная последовательность функционирования скрытого канала и отправки конфиденциальной информации на рабочую станцию нарушителя приведена в виде алгоритмической схемы на рис. 2. Здесь требуемый для передачи объем конфиденциальной информации разбивается на некоторое количество фрагментов определенного размера. Размер каждого фрагмента зависит от того, каким образом будет маскироваться его транспортировка в рамках HTTP/HTTPS обмена. Передача начинается со случайно выбранного фрагмента с номером PN из общего числа N фрагментов.

В данной работе при моделировании такого скрытого канала использовался вариант маскировки передаваемых фрагментов в теле HTTP-запросов GET (URL) в области полей со служебной информацией. Такой запрос однозначно будет правильно обработан прокси-сервером, и при его пересылке за пределы сегмента корпоративной сети к целевому веб-сайту все служебные поля будут сохранены без изменений. Одним из характерных полей, допускающих произвольное содержание, которые сопровождают запрос GET, являются поля “Cookie:”. В этих полях веб-браузер ретранслирует ранее сохраненную и связанную с конкретным веб-сайтом некоторую произвольную информацию [9]. Это давно известный и не вызывающий подозрения способ сохранения данных на стороне веб-браузера в ходе взаимодействия с некоторым веб-сервером, который применяется для хранения персональных предпочтений и настроек пользователя, отслеживания и управление состоянием сеанса доступа и т.п. Такую сохраненную информацию веб-браузер отправляет вместе с остальными служебными заголовками с каждым запросом к веб-серверу. Согласно RFC 6265, размер каждого Cookie не превышает 4096 байт, соответственно предел для каждого фрагмента передаваемой конфиденциальной информации можно установить, исходя из этого значения. Для большей правдоподобности и лучшей маскировки в моделируемом обмене размер фрагмента принят равным 1024 байт. Каждый фрагмент при этом может дополнительно обрабатываться некоторым криптографическим алгоритмом, ответная часть которого известна и имплементирована на стороне нарушителя.

Поля “Cookie:” содержат два элемента cookie, которые используются вредоносным ПО для передачи фрагмента. Элемент “ck_encm” содержит цифровой идентификатор примененного к передаваемому фрагменту метода обработки — номер/индекс криптоалгоритма или иной процедуры кодирования (например, 0 — base64, 1 — AES256, …). Элемент “ck_RNDNAME” является основным элементом cookie, которое содержит передаваемый фрагмент данных. Для усложнения процесса обнаружения имя этого элемента генерируется случайным образом (вместо RNDNAME) и представляет собой строку длиной 6-12 случайных символов латинского алфавита.

Сформированные поля “Cookie:” добавляются к случайно выбранному из банка шаблонов заранее сфор-

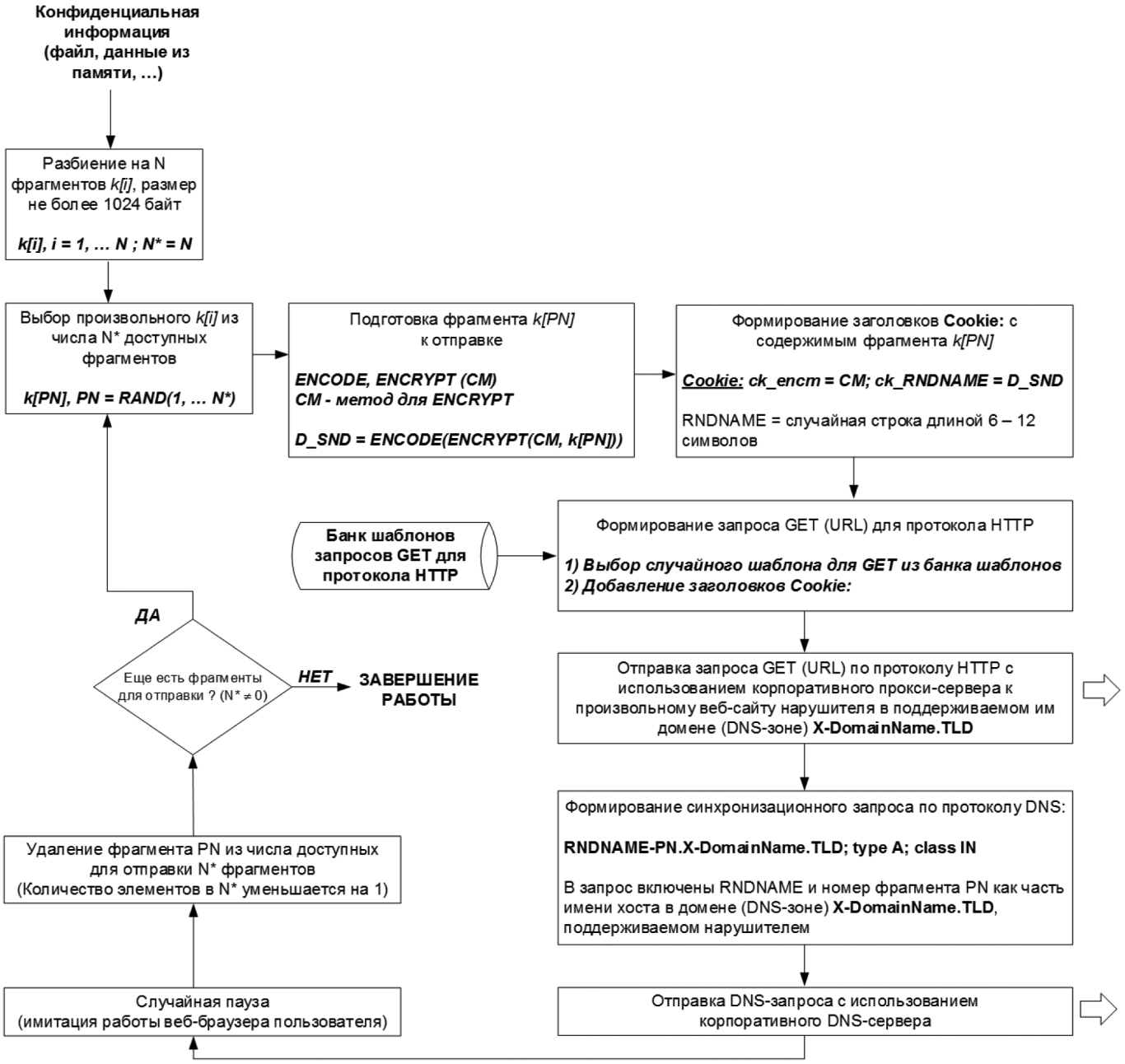

Рис. 2. Алгоритмическая схема работы вредоносного ПО при отправке конфиденциальной информации с рабочей станции

мированных типовых запросов GET (URL) шаблону запроса, который содержит все необходимые служебные поля, сопровождающие такой запрос. В банке шаблонов включены запросы к различным документам и объектам (html-страницы, изображения, pdf-файлы, …) для имитации выполняемого запроса от лица веб-браузера. Готовый запрос с использованием протокола HTTP/HTTPS отправляется через корпоративный прокси-сервер на адрес веб-сайта в домене, контролируемом нарушителем — например, к веб-сайту www.X-DomainName.TLD . Вместо 'www' может использоваться любой другой хост в домене нарушителя. Пример сформированного запроса приведен на рис. 3.

После отправки запроса GET (URL) вредоносное ПО формирует DNS-запрос на получение IP-адреса (A-запись) некоторого хоста в домене нарушителя. В качестве имени хоста используется составная конструкция, включающая в себя случайно сгенерированное имя элемента cookie «ck_RNDNAME» и порядковый номер отправляемого фрагмента PN. Запрос адресуется корпоративному DNS-серверу, который иерархически перенаправляет его (уже от своего адреса) на адрес рабочей станции нарушителя. Таким образом обеспечивается синхронизация и обнаружение на стороне нарушителя ранее переданного фрагмента и сопоставление его порядкового местоположения при составлении оригинального блока конфиденциальной информации.

```
GET /forum/userpage/page1.html HTTP/1.1\r\n
Host: www.X-DomainName.TLD\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Referer: http://www.X-DomainName.TLD/\r\n
Cookie: ck_encm=0; ck_mngexsghy=aGlkZGVuIGNvbmZpZGVudGlhbCBwYXJ0IGh1 ... cmU==\r\n
\r\n
```

Рис. 3. Сформированный HTTP-запрос, содержащий передаваемый фрагмент данных

Работа вредоносного ПО на рабочей станции продолжается до окончания передачи всех фрагментов. При передаче между фрагментами делается случайная пауза.

На рабочей станции нарушителя функционирует ответная часть ПО, имитирующая работу веб-сервера и DNS-сервера. При этом, компонента, отвечающая за получение HTTP-запросов, сохраняет содержимое полей «Cookie:» из полученного запроса, производит анализ содержимого запроса GET (URL) и формирует для обратного отправления ожидаемый ответ — на запрос html-страницы отправляется заранее заготовленное содержимое некоторой html-страницы, на запрос изображения — заранее заготовленное изображение с требуемым MIME-типом (JPG, PNG, …) и т.п. Задача данной компоненты ПО на рабочей станции нарушителя — обеспечивать полную имитацию взаимодействия «веб-браузера» с «веб-сервером». DNS-компонента обеспечивает прием DNS-запросов и извлечение запрашиваемого имени хоста в домене нарушителя из запроса. Ответ выглядит стандартно и содержит IP-адрес рабочей станции нарушителя (или любой другой IP-адрес) для обеспечения полной имитации работы «DNS-сервера».

Полученная синхронизационная информация используется для нахождения нужного фрагмента и упорядочивания извлеченной из него информации. Выполнив все процедуры обработки полученных фрагментов и составив их в правильном порядке, на рабочей станции нарушителя оказывается копия переданного с рабочей станции в корпоративной сети объема конфиденциальной информации.

Компоненты вредоносного ПО для выполнения моделирования и рассмотрения его работы выполнены в виде программного кода на языке Python [10]. Модель сегмента корпоративной сети и участка сети с рабочей станцией нарушителя имитировались в виртуальной лабораторной среде «EVE-NG» [11], которая содержит необходимые виртуальные компоненты сетевых устройств, рабочих станций и специализированных решений защиты информации. Используемые анализаторы трафика абсолютно корректно идентифицируют создаваемый обмен как обмен по протоколам HTTP и DNS, который свободно преодолевает механизмы защиты на границе сегмента корпоративной сети и средства контроля и анализа корпоративного прокси-сервера (выполнен на основе ПО Squid [12] с дополнительными средствами анализа, контроля, фильтрации и антивирусной обработки проксируемого трафика).

Подходы к обнаружению и устранению скрытого канала утечки конфиденциальной информации

Поскольку в работе ранее уже было сказано, что обнаружение подобных каналов является сложной задачей, то логичным представляется решение диверсифицировать подходы к обнаружению и предотвращению возможности успешной работы вредоносного ПО на рабочих станциях внутри защищаемого сегмента корпоративной сети. Если просмотреть весь путь такого скрытого канала, то можно выделить три явных точки, в которых необходимо применить дополнительные средства контроля, анализа и ограничения для блокирования работы скрытого канала. Такими точками являются — сама рабочая станция с вредоносным ПО, корпоративный прокси-сервер как посредник основного канала передачи конфиденциальной информации, и средства контроля на границе корпоративной сети.

1) На рабочих станциях необходимо наличие централизованно администрируемого современного межсетевого экрана следующего поколения (NGFW — Next Generation Firewall) уровня узла [13], позволяющего формировать разрешительные и запретительные правила с учетом порождающего сетевой трафик конкретного приложения и рабочего контекста, что составляет дополнительную метаинформацию, используемую в составе правил фильтрации сетевого трафика. Таким образом, можно будет однозначно определять, каким именно приложениям на рабочей станции можно инициировать сетевой обмен с использованием определенного набора сетевых протоколов. Это позволит исключить возможность установления соединений и организацию сетевого взаимодействия для вредоносного ПО на рабочих станциях корпоративной сети.

2) На корпоративном прокси-сервере с использованием протокола ICAP возможно подключение внешнего решения, которое будет осуществлять детальный анализ служебных полей отправляемых HTTP-запросов и от-

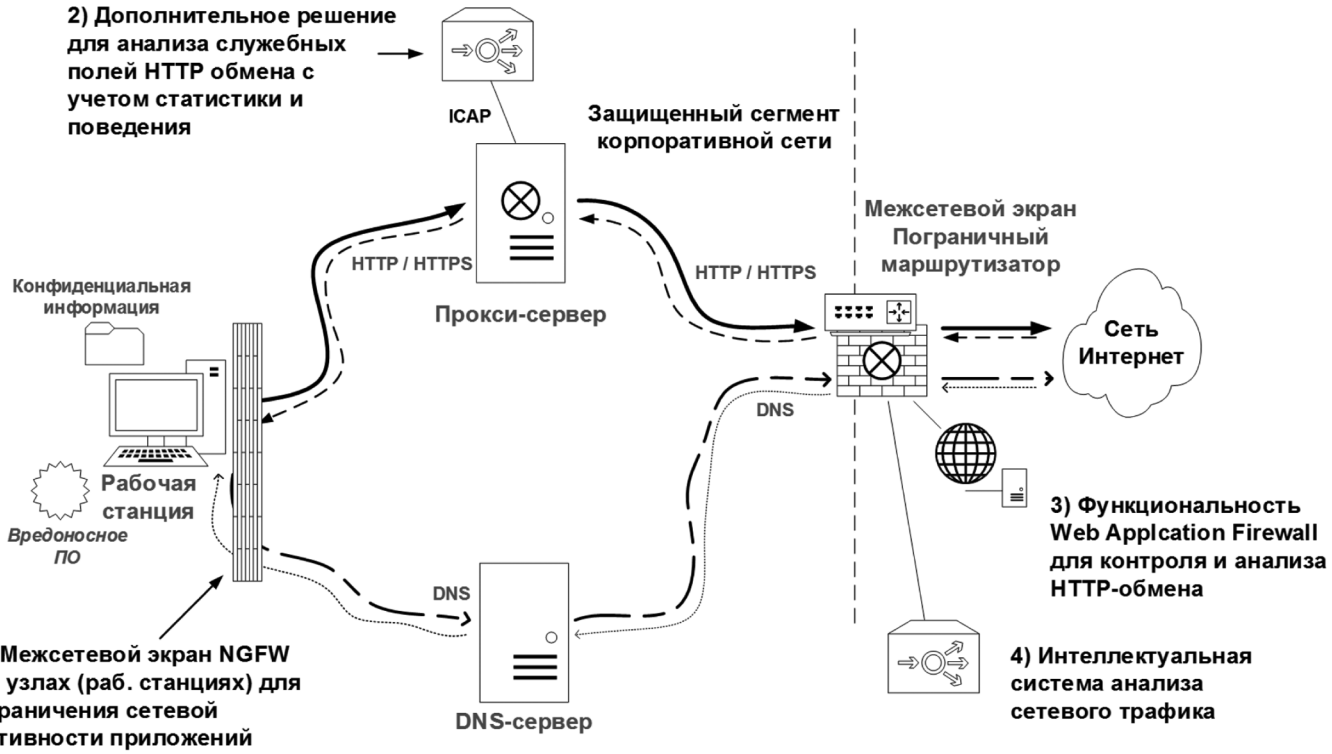

Рис. 4. Применяемые меры по обнаружению и блокировке скрытого канала утечки конфиденциальных данных

ветов. Подобное решение может собирать статистику по различным служебным полям запросов в адрес каждого конкретного веб-сайта (веб-сервера). В этом случае, исключая набор стандартных полей заголовка запроса, определение размера таких дополнительных полей, как «Cookie:», позволит выявить аномалию по общему размеру элементов поля. Согласно исследованию [14], медианный размер элемента поля «Cookie:» составляет 36 байт, а для 99 % процентов случаев не превышает 300 байт. Тогда появление элемента большого размера может служить индикатором возможной аномалии в сетевом обмене.

Кроме этого, для разных запросов к одному и тому же веб-сайту (веб-серверу) набор элементов в поле «Cookie:» и их имена чаще всего сохраняются стабильными и неизменными. Отличающиеся имена элементов поля «Cookie:» также может являться еще одним признаком возможной аномалии.

3) На границе корпоративной сети возможно расширение функциональности межсетевого экрана до уровня, обеспечивающего контроль и фильтрацию информационных потоков по протоколу передачи гипертекста (WAF — Web Application Firewall), проходящих к веб-серверу и от веб-сервера [13]. В этом случае возможно обнаружение аномально больших или часто меняющихся полей «Cookie:» средствами более совершенного межсетевого экрана.

4) На границе корпоративной сети возможно применение интеллектуальной системы анализа сетевого трафика, которая позволит сформировать критерий (правило) для гибридной проверки HTTP-запросов и DNS-запросов, идущих в адрес одного и того же домена, контролируемого нарушителем. Большое количество запросов к DNS-серверу домена, не связанных с именем веб-сервера или серверов в этом домене, может служить индикатором действующей аномалии в корпоративной сети, которая требует вмешательства администратора и специалиста по защите информации.

Сводное представление применяемых мер на защищенном сегменте корпоративной сети приведено на рис. 4.

Заключение

В работе выполнено моделирование и исследование принципов работы потенциального скрытого канала утечки конфиденциальной информации из защищенного сегмента корпоративной сети. Актуальность проблемы подчеркивается тем, что маскировка под популярные прикладные протоколы обмена данными в корпоративной сети и активное использование существующей сетевой инфраструктуры и технологий делает работу такого скрытого канала малозаметной и сложно идентифицируемой, особенно в автоматическом режиме с использованием стандартных решений по защите информации. Проведенное исследование показывает, что алгоритмически работа такого канал совпадает с работой штатных программных средств (веб-браузеров), а применяемые способы включения данных для последующей передачи

используют стандартные функциональные возможности прикладных протоколов. Эти факты указывают на необходимость дополнительных мер и решений по более глубокому анализу сетевого трафика в точках его обработки и на границе сети, так и дополнительных средств по обеспечению безопасности непосредственно самих рабочих станций.

ЛИТЕРАТУРА

1. Код безопасности: Защита корпоративных сетей в России — 2017. Аналитическое исследование. Ноябрь 2017 г. [Электронный ресурс] — Режим доступа — URL: https://www.securitycode.ru/upload/iblock/892/Network_security_2017.pdf/ (дата обращения 25.07.2023)
2. L. Dixon, T. Ristenpart, T. Shrimpton. Network Traffic Obfuscation and Automated Internet Censorship. IEEE Security & Privacy. 2016. V. 14, N. 6, pp. 43–53. DOI: 10.1109/MSP.2016.121.
3. А.В. Закалкин, С.А. Иванов, Е.В. Вершенник, А.В. Кирьянов. Способ маскирования передаваемой информации // Труды ИСП РАН. — 2020 г. — №6. — С. 17–20.
4. H. Moghaddam, B. Li, M. Derakhshani, et al. SkypeMorph: protocol obfuscation for Tor bridges. Proceedings of the 2012 ACM Conference on Computer and Communications Security. 2012. pp. 2–6. DOI: 10.1145/2382196.2382210
5. Z. Weinberg, J. Wang, V. Yegneswaran, et al. StegoTorus: a camouflage proxy for the Tor anonymity system. Proceedings of the 2012 ACM Conference on Computer and Communications Security. 2012. pp. 109–120. DOI: 10.1145/2382196.2382211
6. Q. Wang, X. Gong, G.T.K. Nguyen, et al. Censorspoofer: Asymmetric communication with IP spoofing for censorship-resistant web browsing. // arXiv:1203.1673 [cs.CR]. [Электронный ресурс] — Режим доступа — URL: https://arxiv.org/pdf/1203.1673.pdf (дата обращения 25.07.2023)
7. Р.А. Астаулов. Обнаружение скрытого канала передачи данных по протоколу DNS // Актуальные проблемы авиации и космонавтики. — 2018 г. — №14.— С. 22–30.
8. В.В. Галушка, С.Б. Петренкова, Я.В. Дзюба, В.А. Панченко. Сетевая стеганография на основе ICMP-инкапсуляции // Инженерный вестник Дона. — 2018 г. — №4(51). — С. 107–123.
9. A. Barth. RFC 6265 — HTTP State Management Mechanism. [Электронный ресурс] — Режим доступа — URL: https://www.ietf.org/rfc/rfc6265.txt (дата обращения 25.07.2023)
10. Python. [Электронный ресурс] — Режим доступа — URL: https://www.python.org/ (дата обращения 25.07.2023)
11. EVE-NG. [Электронный ресурс] — Режим доступа — URL: https://www.eve-ng.net/ (дата обращения 25.07.2023)
12. Squid: Optimising Web Delivery. [Электронный ресурс] — Режим доступа — URL: http://www.squid-cache.org/ (дата обращения 25.07.2023)
13. Информационное сообщение ФСТЭК России от 28 апреля 2016 г. N 240/24/1986. [Электронный ресурс] — Режим доступа — URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-28-aprelya-2016-g-n-240-24-1986 (дата обращения 25.07.2023)
14. Analysis of Cookie Size. [Электронный ресурс] — Режим доступа — URL: https://discuss.httparchive.org/t/analysis-of-cookie-size/1991/ (дата обращения 25.07.2023)