УДК 004.492
DOI 10.33764/2618-981X-2022-6-127-133

Обнаружение сетевых закладных устройств в периметре организации

Н. Д. Кульбякина[1], Г. В. Попков[2]*
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: natashaK-2009@mail.ru

Аннотация. Одной из важных задач в обеспечении информационной безопасности корпоративной сети является обеспечение бесперебойной работы ее основных компонентов, особенно в период пиковых нагрузок. Развитие сетевой инфраструктуры неизбежно связано с возникновением в сети процессов, снижающих производительность сети. Одной из сложнейших задач администрирования крупных корпоративных сетей является отслеживание паразитного трафика, создаваемого компьютерными вирусами, различными сканерами и программным обеспечением. Кибергруппировки преодолевают защиту на периметре интересующих их организаций, и об этом свидетельствует тенденция к росту доли успешных целевых атак. Это повод сместить фокус внимания с предотвращения атак на периметре на своевременное выявление компрометации и реагирование внутри сети. Однако выявить тщательно спланированную, порой разнесенную во времени кибератаку сложно. Тем не менее действия взломщиков оставляют следы в сетевом трафике, а значит, задача специалиста по кибербезопасности — обнаружить эти следы. В данной статье будет рассмотрен один из возможных вариантов, как выявить нетипичную сетевую активность и обнаружить конечное устройство, которое генерирует данные события.

Ключевые слова: сеть, сетевая безопасность, паразитный трафик, системы обнаружения вторжений (Zeek)

Detection of network embedded devices in the perimeter of the organization

N. D. Kulbyakina[1], G. V. Popkov[2]*
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
*e-mail: natashaK-2009@mail.ru

Abstract. One of the important tasks in ensuring the information security of a corporate network is to ensure the smooth operation of its main components, especially during peak loads. The development of network infrastructure is inevitably associated with the emergence of processes in the network that reduce network performance. One of the most difficult tasks in the administration of large corporate networks is tracking parasitic traffic generated by computer viruses, various scanners and software. Cyber groups are overcoming the protection on the perimeter of the organizations they are interested in, and this is evidenced by the trend towards an increase in the proportion of successful targeted attacks. This is an occasion to shift the focus from preventing attacks on the perimeter to timely detection of compromise and response within the network. However, it is difficult to identify a carefully planned, sometimes time-spaced cyberattack. Nevertheless, the actions of hackers leave traces in network traffic, which means that the task of a cybersecurity specialist is to detect these

traces. This article will consider one of the possible options for identifying atypical network activity and detecting the end device that generates these events.

Keywords: network, network security, parasitic traffic, intrusion detection systems (Zeek)

Введение

Основная опасность сетевых закладных устройств (под сетевым закладным устройством имеется ввиду любое устройство, имеющее сетевой интерфейс и способное подключится к сети Интернет) заключается в том, что, являясь частью защищенной системы, они способны принимать активные меры по маскировке своего присутствия в системе. При внедрении в систему закладки в защищенной системе создается скрытый канал сетевого обмена, который, как правило, не всегда удаётся выявить сразу. Большая часть закладных устройств, применявшиеся в разное время, были выявлены либо из-за ошибок, допущенных при программировании закладки, либо случайно.

Если закладка имеет грамотно написанный программный код, то после того, как она внедрена в систему, обнаружить ее стандартными средствами администрирования очень трудно, поэтому она может функционировать неограниченно долгое время, – и на протяжении всего этого времени внедривший ее злоумышленник имеет практически неограниченный доступ к системным ресурсам.

Закладки могут наносить ущерб как отдельным пользователям и компаниям, так и целым государствам, например, ставя под угрозу обороноспособность страны.

В рамках статьи будет рассмотрен стандартный инструментарий по исследованию и выявлению нетипичных сетевых активностей: система обнаружений вторжений Zeek и сниффер трафика Wireshark. Для корректного использования инструментов была детально изучена официальная документация [1, 2].

Целью статьи является выявление паразитной нагрузки в корпоративной сети и поиска конечного источника, который инициирует соединения с внешним сервером, выполняющим функцию командного сервера для вредоносного программного обеспечения.

Методика исследования

Для достижения поставленной цели необходимо произвести анализ сетевого трафика [3] и выявить подозрительные внешние соединения: для данной задачи будет использован сниффер трафика Wireshark. Программный продукт позволяет перехватывать входящие и исходящие TCP-пакеты и выявлять сетевые ошибки и аномалии [4], что упрощает работу сетевых администраторов и службы информационной безопасности при расследовании инцидентов. После того, как выявлены нетипичные соединения, необходимо более подробно изучить их причину, для этого будут применены специальные фильтры в программе Wireshark, которые дадут возможность изучить передаваемый сетевой пакет и определить причины их возникновения [5].

Далее, когда обнаружен IP-адрес внутреннего зараженного источника, необходимо определить точное название рабочей станции, так как ip-адреса назначаются автоматически и время от времени меняются. Для этого будет использо-

ваться сетевая система обнаружений вторжений (далее - IDS) Zeek [6]. Zeek – это ведущий в мире инструмент пассивного мониторинга сетевой безопасности, который внедрен в сеть и считывает весь трафик, проходящий через сеть, разбирает его на высокоуровневые события и генерирует полный лог каждого соединения, видимого в сети, включая все HTTP сессии с их запрошенными URI, ключевыми заголовками, MIME типами и ответами сервера; DNS запросы с ответами; SSL сертификаты; ключевое содержимое SMTP сессий и т.д. [7]. Имя рабочей станции будет выявлено как раз через анализ одного из имеющихся журналов событий, которые Zeek записывает в реальном времени или же в период анализа файла с расширением pcap.

В заключении будут представлены некоторые рекомендации для избежания похожих случаев в будущем.

Выявление закладных устройств в локальной сети

Основным способом выявления закладных устройств является наличие паразитного (нежелательного) сетевого трафика. Источниками такого трафика могут выступать: различные сетевые сканеры, компьютерные вирусы, соединения программного обеспечения (например, Adobe, Microsoft поддерживают постоянное соединение с серверами обновлений) и несанкционированное использование сетевых точек (отсутствие парольной защиты на Wi-Fi роутере) [8].

В рамках этой статьи вредоносным будем считать трафик, который генерируется вредоносным программным обеспечением в локальной сети. Вредоносность такому сетевому взаимодействию придают передаваемые по сети данные, которые обеспечивают корректную работу вредоносного программного обеспечения (ВПО) и могут влиять на одну из характеристик информации, которая хранится и обрабатывается в системе, а именно: целостность, доступность, конфиденциальность [9].

ВПО в большинстве случаев генерирует в сети следующую информацию:

– отчет о инфицировании системы;

– собранные в системе учетные данные;

– принимаемые команды от управляющего сервера;

– загружаемые модули обновления ВПО;

– сетевой трафик, который используется для атак DDoS.

Для обнаружения вредоносного сетевого взаимодействия необходимо иметь возможность записывать фрагменты сетевого взаимодействия для их дальнейшего анализа (в статье для данной цели будет использован сниффер трафика Wireshark). Далее для обогащения информацией и выявления конечного зараженного источника будет использована IDS Zeek.

Для начала необходимо произвести запуск Wireshark и проанализировать текущие соединения в корпоративной сети (рис. 1).

Допустим, были обнаружены постоянные соединения со сторонним IP-адресом, находящимся во внешней сети, который кажется подозрительным и неприемлемым, согласно политике компании. В интерфейсе Wireshark подозри-

тельные взаимодействия в основном выявляют по количеству проходящей информации от одного сетевого источника к другому (рис. 2).

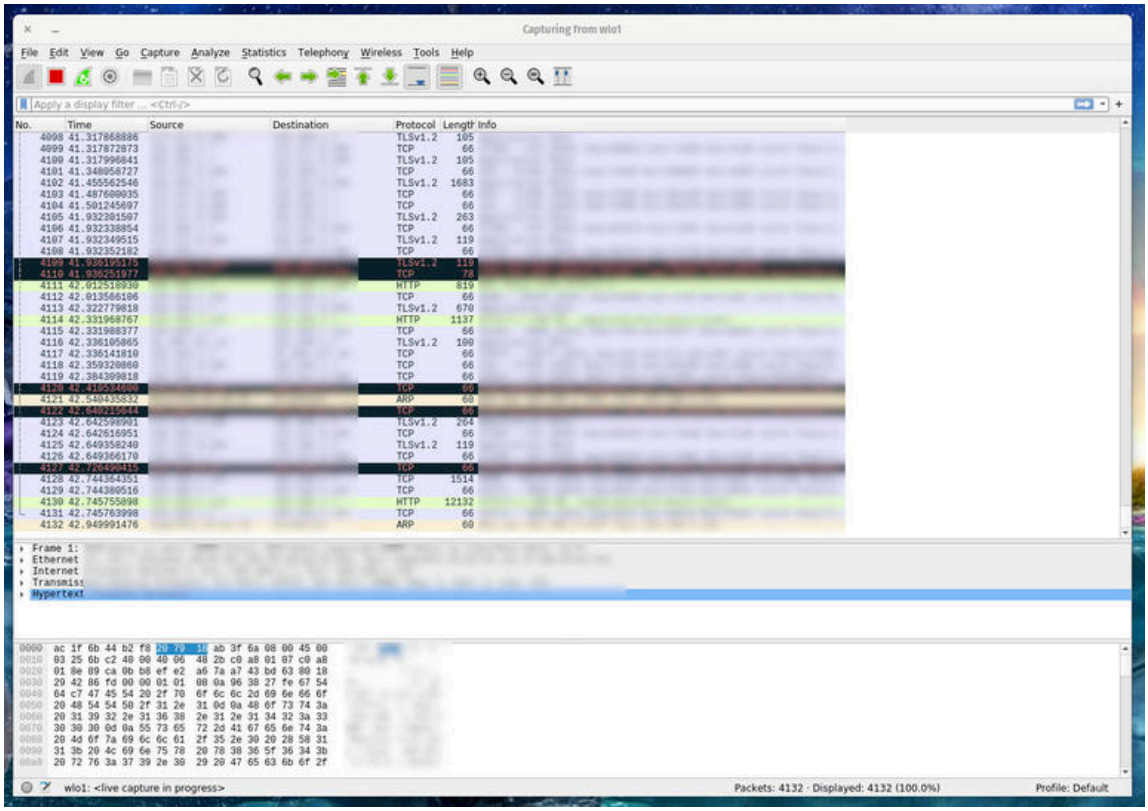

Рис. 1. Интерфейс и просмотр трафика Wireshark

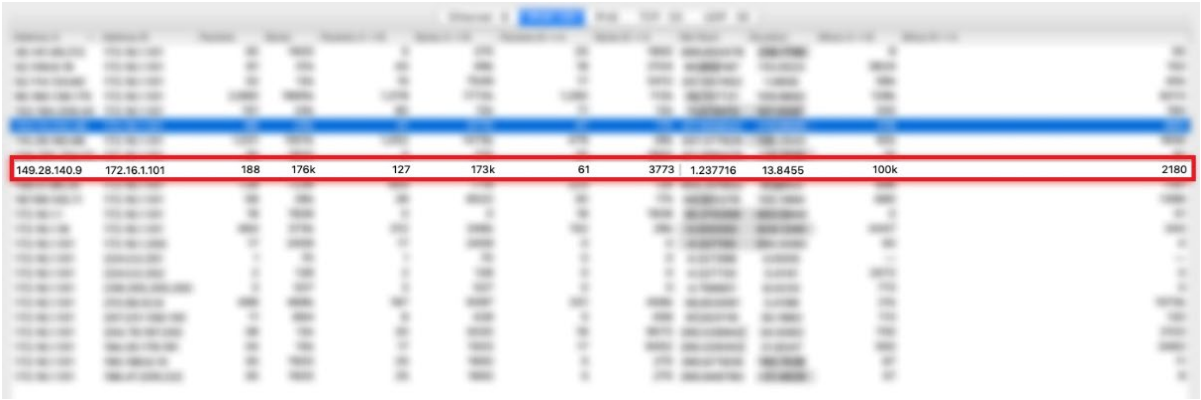

Рис. 2. Выявление подозрительного трафика в сети

Подозрительными выглядят соединения с IP-адресом 149.28.140.9, выставим фильтр Wireshark: ip.addr==172.16.1.101 && tcp.port==65483 && ip.addr==149.28.140.9 && tcp.port==80 [2]. После этого удалось выявить как хост из внутренней сети инициировал соединение с ранее выявленным IP-адресом, также удалось извлечь доменное имя вредоносного источника, с которым осуществляется соединение (рис. 3).

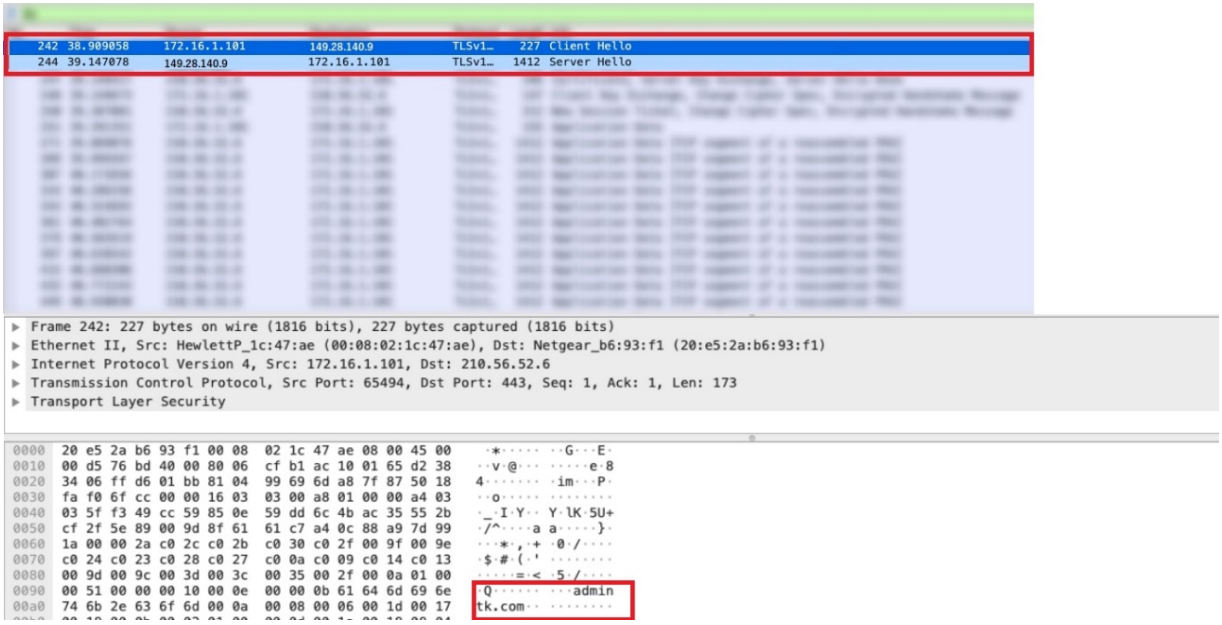

Рис. 3. Выявление соединений с внешним IP - адресом

Помимо коннекта удалось перехватить сетевой пакет с полезной нагрузкой (рис. 4).

Рис. 4. Пакет с полезной нагрузкой № 1. Загрузка шаблона Normal.dotm

Обнаружено, что на устройстве открыт документ, который подгружает файл шаблона для документа MS Office. Далее был найден обфусцированный скрипт на VBA (рис. 5).

Таким образом, можно сделать вывод, что выявленное взаимодействие – это этап инфицирования ОС вредоносным программным обеспечением.

Рис. 5. Пакет с полезной нагрузкой. Обфусцированный VBA - код

Следующим шагом необходимо установить точное имя зараженного хоста внутри сети по его IP-адресу. Для этого сохраним записанный трафик в Wireshark в файл potential_malware.pcap и проанализируем его с помощью IDS Zeek, запустим в терминале следующую команду [10]:

zeek -r potential_malware.pcap -C.

После её выполнения в соответствующей директории будут созданы журналы логов. Для того чтобы узнать точный хост, который инициировал соединение с внешним источником, необходимо открыть журнал dhcp.log со следующими фильтрами: IP-адрес источника и ключ client_fqdn (отвечает за доменное имя устройства в сети):

cat dhcp.log | zeek-cut client_addr client_fqdn.

Вывод команды следующий:

172.16.1.101 LAPTOP-4GL8J5UN.

Заключение

Таким образом был точно установлен зараженный хост, далее необходимо оперативно приступить к локализации последствий от заражения ВПО, выявить остальные источники, которые возможно также были скомпрометированы.

После расследования сотрудник службы информационной безопасности должен принять все возможные соответствующие меры во избежание подобных случаев в будущем. Например, настроить или произвести обновление сигнатур антивирусного программного обеспечения, настроить журналы мониторинга с конечных устройств пользователей и имеющихся средств защиты, чтобы реа-

гирование на инцидент было более оперативным и зараженный хост был вовремя изолирован из общей корпоративной сети, установить или произвести детальную настройку межсетевых экранов – данная мера позволит блокировать паразитные IP-адреса и устанавливать соединения только с источниками, которые отражены в белом списке.

Все вышеописанные меры подойдут небольшой организации, корпоративная сеть которой не была оснащена средствами защиты информации от утечек и заражения ВПО.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Официальная документация IDS Zeek [Электронный ресурс]. URL: https://docs.zeek.org/en/master/index.html (дата обращения: 14.03.2022).

2. Официальная документация сниффера трафика [Электронный ресурс]. URL: Wireshark https://www.wireshark.org/docs/wsug_html/ (дата обращения: 05.04.2022).

3. Милославсая Т.Г. Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: автореферат диссертации на соискание ученой степени доктора технических наук / Милославская Наталья Георгиевна; Федеральный исследовательский центр «Информатика и управление» Российской академии наук – Москва, 2020. – 40 с. – Библиогр.: с. 37–40. – Текст: автореф.дис.

4. Милославская, Н.Г. Визуализация процессов управления информационной безопасностью / Наталья Геннадьевна Милославская // Научная визуализация. - 2017. - Том 9, № 5. - С. 117-136. (дата обращений 01.05.2022).

5. ГОСТ Р «Защита информации. Мониторинг информационной безопасности. Общие положения». Проект [Электронный ресурс]: Веб-сайт / ФСТЭК России. - Режим доступа: https://fstec.ru/tk-362/standarty-tk362/303-proekty/1896-proekt-natsionalnogo-standarta-gost-r-4 (дата обращения: 17.04.2022).

6. Воронина А.А., Скрипина И.И. Предупреждение инцидентов нарушения информационной безопасности данных // Научный результат. Информационные технологии. – Т.6, №3, 2021. – С. 20-25.

7. Вьющенко О.О., Маслова М.А. Об обеспечении безопасности в сфере интернета вещей // Научный результат. Информационные технологии. – Т.6, №3. – С. 33-39.

8. Ревенков П.В., Бердюгин А.А. Кибербезопасность в условиях интернета вещей и электронного банкинга // Национальные проекты: приоритеты и безопасность. – 2016, № 11.–С.158-169.

9. Вишняков Я.Д., Харченко С.А. Управление обеспечением безопасности предприятий: экономические подходы // Менеджмент в России и за рубежом. - №5, 2019 (дата обращения: 02.05.2022).

10. Гибилинда Р. В. Разработка автоматизированных методов анализа воздействий на файлы в задаче расследования инцидентов информационной безопасности: автореферат диссертации на соискание ученой степени кандидата технических наук / Гибилинда Роман Владимирович; учебно-научный центр «Информационная безопасность» Института радиоэлектроники и информационных технологий - РтФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина», Екатеринбург - 2021. – 21 с. – Библиогр.: с. 16–29. – Текст: автореф.дис (дата обращения: 02.05.2022).