УДК 004.056 Вестник УрФО № 4(34) / 2019, с. 58–62

Пырьев М. С., Коллеров А. С.

DOI: 10.14529/secur190407

СРЕДСТВА АНАЛИЗА СЕТЕВОГО ТРАФИКА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ В РЕТРОСПЕКТИВЕ

В статье рассмотрена проблема обнаружения распределенной по времени сетевой атаки. Проанализированы отчёты о состоянии безопасности информационного пространства от Лаборатории Касперского и IBM Security, а также выявлены этапы ретроспективного анализа сетевого трафика на основе исследований в области компьютерной криминалистики. Были выдвинуты предположения о возможных проблемах на каждом этапе и предложены пути решения. Исследованы существующие системы анализа сетевого трафика, используемые для решения существующей проблемы, проведена сравнительная характеристика и выявлена их ограниченность.

Ключевые слова: *инцидент информационной безопасности, ретроспектива, система анализа трафика, компьютерная криминалистика, сбор доказательств, вредоносная активность.*

Pyr'ev M. S., Kollerov A. S.

RETROSPECTIVE ANALYSIS TOOLS OF LOCAL AREA NETWORK TRAFFIC

The article considers the problem of detecting a time-distributed network attack. Reports on the state of information space security from Kaspersky Lab and IBM Security are analyzed, as well as stages of a retrospective analysis of network traffic based on research in the field of computer forensics are identified. Assumptions were made about possible problems at each stage and solutions were proposed. Existing network traffic analysis systems used to solve the existing problem are investigated, a comparative description is made and their limitations are revealed.

Keywords: *information security incident, retrospective, traffic analysis system, computer forensics, evidence collection, malicious activity.*

Первоначально, при выборе пути исследования необходимо отталкиваться от фактора полезности данного исследования для общества. Так, область для изучения была выбрана исходя из определения значимости ущерба в случае вмешательства злоумышленника в работу какой-либо отрасли. Наибольший ущерб от данных действий полагается на промышленный сектор, конкретнее – при нарушении работы автоматизированных систем управления (АСУ).

Даже защищенная сеть АСУ может быть атакована, так как существуют неучтенные уязвимости (или же уязвимости «нулевого

дня»), которые выявляются путем тщательного исследования. В связи с этим, крайне необходимо отслеживать и контролировать процессы, протекающие внутри компании или предприятия.

Также, по статистике процентное содержание целевых атак с каждым годом возрастает, что свидетельствует о подготовленности злоумышленников.

Так, доля атакованных средств вычислительной техники АСУ в первом полугодии 2018 в мире выросла на 3,5 п.п. и составила 41,2%. За год этот показатель закрепился на уровне 41%, что свидетельствует о том, что каждый третий компьютер на производстве подвергается атаке.

Рост процента атакованных компьютеров АСУ связан, в основном, с общим повышением вредоносной активности. [2, 3]

Немаловажно учесть тот момент, что инцидентов не избежать, однако можно снизить их количество. Данным вопросом занимается сетевая форензика.

Назначение сетевой форензики:

• детальное исследование сетевой инфраструктуры, работы различных программ, в том числе вирусной активности;

• мониторинг сетевых инцидентов, оставляемых следов, инструментов совершения мошеннических действий;

• сбор доказательств для ведения расследования в компьютерной криминалистике;

• отслеживание источников сетевых атак и т.д.

Принцип действия систем сетевой форензики строится на сборе и анализе больших объемов неструктурированных данных.

С помощью технологии сетевой форензики у ИТ-специалистов и офицеров информационной безопасности появляется возможность наглядно рассмотреть всю сетевую инфраструктуру компании вне зависимости от ее размера, отобразить действия всех пользователей, обнаружить подозрительную аномальную активность в сети, включая кибератаки различной мощности, и при получении оповещения оперативно осуществить реакцию, например, ликвидировать последствие атаки. При этом благодаря воспроизведению записи трафика и ретроспективному анализу детально расследовать сетевые инциденты, устранять уязвимости инфраструктуры можно еще до появления разрушительных и критических последствий, а также собрать исчерпывающую доказательную базу для защиты интересов компании от внутренних и внешних угроз. [4]

Криминалистический процесс, который проводят специалисты и эксперты, принято делить на четыре этапа [5]:

1) сбор;

2) исследование;

3) анализ;

4) представление.

Первый, третий и четвертый этапы в большинстве случаев имеют четкие инструкции по их проведению, в тоже время, второй этап, включающий механизм считывания информации с носителей и особенно вычленения из нее той, которая относится к делу, наименее формализован и вызывает трудности при проведении экспертного исследования собранной информации.

Рассмотрим подробнее второй этап представленного процесса.

Для автоматизации процессов исследования применяют системы анализа сетевого трафика.

Системы анализа трафика можно классифицировать по типу работы на:

• системы, работающие в режиме реального времени;

• ретроспективные системы.

К первым относятся системы обнаружения вторжений, контроля утечек информации, то есть для постоянного мониторинга защищенности сети.

Ретроспективный анализ заключается в процессе записи трафика и последующего его анализа на предмет источника инцидента ИБ, если такой имеется. Кроме того, данный анализ может привести к выявлению планируемой атаки, так как по данным исследования Ponemon Institute [11] среднее время присутствия злоумышленника в инфраструктуре атакованной организации – 206 дней.

Исходя из повышения развития сетевых инфраструктур в жизни общества, а также нестандартности мышления злоумышленников ретроспективный анализ наиболее актуален для исследований и внедрения в системы обеспечения ИБ объектов защиты, так как позволяет проводить обзор всей хронологии событий, выявлять истинную причину возникновения инцидентов, а также выявлять в ходе аудита аномалии в трафике, которые могут являться первопричиной последующих сетевых атак.

Рассмотрим процесс ретроспективного анализа полноценно.

Первоначально, происходит накопление трафика с помощью зеркалирования на интерфейс хранилища. Возможные проблемы на данном этапе:

• недостаточное место для хранения;

• низкая пропускная способность.

Результаты сравнения представлены в таблице 1.

Исходя из полученных результатов, можно заметить, что большинство систем являются закрытыми для изменений решениями, которые сложно адаптировать для выявле-

Таблица 1

Сравнительная характеристика систем анализа сетевого трафика

Название\Критерий	1	2	3	4	5	6
Tcpdump	+	+	-	-	+	-
SolarWinds NTA	-	-	+	-	-	+
ГАРДА Монитор	-	-	+	-	+	+
ntopng	+	+	-	+	-	+
PT Network Attack Discovery	-	-	+	+	+	+
Malcolm	+	+	+	+	+	+

Первый пункт решается установкой необходимой системы хранения данных. Для решения вопроса ретроспективного анализа необходимо хранилище объемом не менее 100 Тб [9].

Второй пункт решается определением пиковой скорости потока данных, установкой канала, превышающего пиковую скорость не менее, чем в два раза, так как трафик будет поступать как входящий, так и исходящий.

Следующим шагом является анализ накопленных данных. Данный этап является ключевым, в рассматриваемой теме. Реализация второго этапа требует обеспечение возможности работы с большим набором неструктурированной информации.

Проведем сравнительную характеристику существующих систем данного класса.

Рассмотрим шесть наиболее популярных решений [1]:

• Tcpdump [6];

• NetFlow Traffic Analyzer [8];

• ГАРДА Монитор [9];

• ntopng [10];

• PT Network Attack Discovery [7];

• Malcolm [12].

Сравнение систем анализа сетевого трафика проводилось по следующим критериям:

1. Открытый исходный код.

2. Возможность некоммерческого использования.

3. Удобство использования для аудитора.

4. Наличие API.

5. Возможность проиграть накопленный трафик в анализаторе.

6. Исследование протоколов прикладного уровня.

ний новых угроз безопасности. В тоже время, решение Malcolm является наиболее подходящим для создания универсальной системы ретроспективного анализа, так как состоит из множества инструментов, распространяемых по свободной лицензии.

Открытый исходный код, наличие API к каждому модулю, простой и понятной к нему документации – ключевые факторы, которые поспособствовали выбору данного решения. Однако, при детальном разборе данной системы, эмпирическим путем было выявлено, что возможности продукта Malcolm с одной стороны избыточны, с другой стороны недостаточны.

Избыточность системы заключается в большом выборе инструментов для аудитора, что создает ситуацию дублирования реализуемых функций в разном графическом исполнении.

Недостаточность системы заключается в ограниченности анализируемых протоколов и отсутствие анализа шифрованного трафика на предмет соответствия политики безопасности.

Финальный этап ретроспективного анализа – отчетность в виде графиков и индикаторов, позволяющих дать оценку ситуации.

Представление на интерфейсе Malcolm информативно и позволяет ретроспективно анализировать обстановку. Однако, исходя из избыточности компонентов данного продукта, возможно сократить функционал до необходимого по данной задаче, тем самым уменьшить время развертывания системы, быстродействие и занимаемую память. Несомненно, необходимо устранить недостаточность ре-

шения путем разработки программного модуля, способного выявить вредоносную активность в зашифрованном сетевом трафике и настроить индикацию данного процесса.

Немаловажен и тот факт, что на данный момент отсутствует методика выявления из визуализации сетевой информации подозрительную, вредоносную или потенциально вредоносную активность.

Таким образом, все рассмотренные системы позволяют анализировать большой объем трафика на высокой скорости, но необходимо обеспечивать визуализацию и осуществлять корреляцию полученных данных, а также выделить из полученных данных подозрительную активность. К тому же, решение должно быть гибкое и независимое. Ближе всего к решению поставленной задачи оказался продукт Malcolm, благодаря его модульной структуре. Реорганизация и фильтрация используемых инструментов поможет увеличить производительность и уменьшить ресурсоемкость, а создание дополнительного модуля позволит представит индицировать аудитору факт нарушения политики безопасности в зашифрованном трафике. Данные изменения поспособствуют автоматизации процесса исследования и снизят временные затраты на проведение анализа ситуации в компании или предприятии.

Литература

1. Пырьев М.С., Коллеров А.С. Ретроспективный анализ сетевого трафика локальной вычислительной сети // Сборник трудов XVIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства». – Магнитогорск : Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2019. – С. 302–306 – ISBN 978-5-9967-1764-4.

2. Ландшафт угроз для систем промышленной автоматизации: первое полугодие 2018 [Электронный ресурс] // Официальный сайт компании «Лаборатория Касперского». URL: https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/#_Toc523499579 (дата обращения: 10.09.2019).

3. Ландшафт угроз для систем промышленной автоматизации: первое полугодие 2019 [Электронный ресурс] // Официальный сайт компании «Лаборатория Касперского». URL: https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (дата обращения: 11.09.2019).

4. Шкарин, Антон. Сетевая форензика – расследование инцидентов в сети предприятия [Электронный ресурс] / А. Шкарин // Информационная безопасность. 2016. №4. С. 50-51. URL: http://lib.itsec.ru/articles2/in-ch-sec/setevaya-forenzika-rassledovanie-intsidentov-v-seti-predpriyatiya (дата обращения: 15.09.2019).

5. Федотов Н.Н. Форензика – компьютерная криминалистика – Москва : Юридический Мир, 2007. – 360 с. – ISBN 5-91159-015-8.

6. Документация tcpdump [Электронный ресурс] // Официальный сайт «Tcpdump/Libpcap». URL: https://www.tcpdump.org/manpages/tcpdump.1.html (дата обращения: 26.09.2019).

7. Описание характеристик PT Network Attack Discovery [Электронный ресурс] // Официальный сайт компании «Positive Technologies». URL: https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/ (дата обращения: 26.09.2019).

8. Описание характеристик анализатора трафика NetFlow [Электронный ресурс] // Официальный сайт компании «SolarWinds». URL: https://www.solarwinds.com/netflow-traffic-analyzer (дата обращения: 09.10.2019).

9. Описание характеристик Гарда Монитор [Электронный ресурс] // Официальный сайт компании «Гарда Технологии». URL: https://www.gardatech.ru/produkty/monitor/ (дата обращения: 09.10.2019).

10. Описание характеристик ntopng [Электронный ресурс] // Официальный сайт компании «ntop». URL: https://www.ntop.org/products/traffic-analysis/ntop/ (дата обращения: 09.10.2019).

11. IBM Security, The data breach lifecycle [Электронный ресурс] / IBM Security // Cost of a Data Breach Report. 2019. P.49-54. URL: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf (дата обращения: 29.11.2019).

12. Описание набора инструментов Malcolm [Электронный ресурс] // Репозиторий на вебсервисе для хостинга IT-проектов «GitHub». URL: https://github.com/idaholab/Malcolm (дата обращения: 01.12.2019).

References

1. Pyr'ev M.S., Kollerov A.S. Retrospektivnyy analiz setevogo trafika lokal'noy vychislitel'noy seti [Retrospective analysis of network traffic on a local area network] // Sbornik trudov XVIII Vseros-siyskoy

nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh «Bezopasnost' informatsionnogo prostranstva» [Proceedings of the XVIII All-Russian Scientific and Practical Conference of Students, Graduate Students and Young Scientists «Information Space Security»]. Magnitogorsk, Izd-vo Magnitogorsk. gos. tekhn. un-ta im. G.I. Nosova, 2019, pp. 302–306. ISBN 978-5-9967-1764-4.

2. Threat Landscape for Industrial Automation Systems: First Half of 2018 [Landshaft ugroz dlya sistem promyshlennoy avtomatizatsii: pervoe plugodie 2018]. Available at: https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/#_Toc523499579 (accessed 10 September 2019).

3. Threat Landscape for Industrial Automation Systems: First Half of 2018 [Landshaft ugroz dlya sistem promyshlennoy avtomatizatsii: pervoe plugodie 2019]. Available at: https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (accessed 11 September 2019).

4. Shkarin A. Network Forensics – Investigation of Incidents in the Enterprise Network [Setevaya forenzika – rassledovanie intsidentov v seti predpriyatiya]. Journal of Information Security, 2016, no.4, pp. 50-51. (in Russian) Available at: http://lib.itsec.ru/articles2/in-ch-sec/setevaya-forenzika-rassledovanie-intsidentov-v-seti-predpriyatiya (accessed 15 September 2019).

5. Fedotov N.N. Forenzika – komp'yuternaya kriminalistika [Computer Forensics]. Moskow, Yuridicheskiy Mir, 2007. 360 p. ISBN 5-91159-015-8.

6. Dokumentacija tcpdump [Manual Page of TCPDUMP]. Available at: https://www.tcpdump.org/manpages/tcpdump.1.html (accessed 26 September 2019).

7. Opisanie kharakteristik PT Network Attack Discovery [PT Network Attack Discovery Feature Description]. Available at: https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/ (accessed 26 September 2019).

8. Opisanie kharakteristik analizatora trafika NetFlow [NetFlow Traffic Analyzer Feature Description]. Available at: https://www.solarwinds.com/netflow-traffic-analyzer (accessed 09 October 2019).

9. Opisanie kharakteristik Garda Monitor [Garda Monitor Feature Description]. Available at: https://www.gardatech.ru/produkty/monitor/ (accessed 09 October 2019).

10. Opisanie kharakteristik ntopng [Ntopng Feature Description]. Available at: https://www.ntop.org/products/traffic-analysis/ntop/ (accessed 09 October 2019).

11. IBM Security, The Data Breach Lifecycle. Cost of a Data Breach Report. 2019, pp.49-54. Available at: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Re-port_final.pdf (accessed 29 November 2019).

12. Opisanie nabora instrumentov Malcolm [Malcolm Toolkit Description]. Available at: https://github.com/idaholab/Malcolm (accessed 01 December 2019).

ПЫРЬЕВ Михаил Сергеевич, студент радиотехнического факультета Института радиоэлектроники и информационных технологий - Уральского Федерального Университета им. Первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19, E-mail: mihail.pyrev@gmail.com

КОЛЛЕРОВ Андрей Сергеевич, кандидат технических наук, доцент Института радиоэлектроники и информационных технологий - Уральского Федерального Университета им. Первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: rtfstudent@gmail.com

PYR'EV Mikhail Sergeevich, student of Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: mihail.pyrev@gmail.com

KOLLEROV Andrey Sergeevich, candidate of technical sciences, associate Professor Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: rtfstudent@gmail.com