УДК 004.056
DOI

ПОДХОДЫ К ОБНАРУЖЕНИЮ И РАССЛЕДОВАНИЮ СЕТЕВЫХ АТАК С ПРИМЕНЕНИЕМ СИСТЕМ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Фейламазова С. А. ORCID ID 0000-0002-2290-2916,
Абдуразакова З. Ш. ORCID ID 0009-0009-4769-3776,
Муртузалиева А. А. ORCID ID 0009-0007-6236-7552

Федеральное государственное бюджетное образовательное учреждение высшего образования «Дагестанский государственный университет», Махачкала, Российская Федерация, e-mail: konspirator13@mail.ru

В статье исследованы возможности и практическое применение открытой платформы анализа сетевого трафика Arkime для обнаружения и расследования кибератак. Выбор платформы Arkime обоснован ее способностью к глубокому ретроспективному анализу и визуализации активности. Цель исследования – оценить возможности и продемонстрировать практическое применение открытой платформы Arkime для обнаружения и расследования сетевых атак. Исследование построено на постинцидентном анализе готовых файлов сетевого трафика, содержащих записи реальных атак. Исследования проведены в тестовой среде на базе операционных систем Ubuntu, Windows 11 и Windows Server. С хоста-анализатора Ubuntu были направлены заранее записанные пакеты атак через сетевой интерфейс на целевые хосты Windows и одновременно захватывались сенсорами Arkime для последующего анализа. Рассмотрены различные сценарии работы системы на примере имитации атак, проведенных в тестовых режимах, и мониторинга хостов на предмет нежелательных действий. Платформа Arkime эффективно выявила компрометации на основе сигнатурного анализа, обнаружила аномальную активность, характерную для взаимодействия с командными серверами вредоносного программного обеспечения, а также идентифицировала передачу вредоносных файлов благодаря интеграции с внешними источниками угроз. Продемонстрированы ключевые возможности Arkime: глубокий анализ метаданных и полезной нагрузки трафика, поиск по индикаторам компрометации, а также наглядная визуализация сетевых событий с помощью настраиваемых дашбордов, что существенно упрощает анализ и расследование инцидентов.

Ключевые слова: сетевой трафик, анализ трафика, расследование инцидентов, Arkime, ретроспективный анализ

APPROACHES TO DETECTING AND INVESTIGATING NETWORK ATTACKS USING NETWORK TRAFFIC ANALYSIS SYSTEMS

Feylamazova S. A. ORCID ID 0000-0002-2290-2916,
Abdurazakova Z. Sh. ORCID ID 0009-0009-4769-3776,
Murtuzalieva A. A. ORCID ID 0009-0007-6236-7552

Federal State Budgetary Educational Institution of Higher Education "Dagestan State University", Makhachkala, Russian Federation, e-mail: konspirator13@mail.ru

The article explores the capabilities and practical application of the open-source network traffic analysis platform Arkime for detecting and investigating cyberattacks. The choice of the Arkime platform is based on its ability to perform in-depth retrospective analysis and visualization of network activity. The purpose of this study is to evaluate the capabilities and demonstrate the practical application of the open-source Arkime platform for detecting and investigating network attacks. The research was conducted in a test environment based on Ubuntu, Windows 11, and Windows Server operating systems. Pre-recorded attack packets were sent from the Ubuntu analyzer host through the network interface to the target Windows hosts and simultaneously captured by the Arkime sensors for subsequent analysis. Various scenarios of the system operation are considered on the example of imitation of attacks carried out in test modes and monitoring of hosts for undesirable actions. The Arkime platform effectively identified compromises based on signature analysis, detected abnormal activity typical for interaction with command servers of malicious software, and also identified the transfer of malicious files due to integration with external sources of threats. Arkime's key capabilities were demonstrated: deep analysis of traffic metadata and payload, search for indicators of compromise, and clear visualization of network events using customizable dashboards, significantly simplifying incident analysis and investigation.

Keywords: network traffic, traffic analysis, incident investigation, Arkime, retrospective analysis

Введение

Рост числа и сложности сетевых атак на фоне геополитической нестабильности повышает спрос на эффективные средства обнаружения угроз.

Современные open-source решения, такие как Arkime, Zeek, Suricata и Wazuh, обладают широким набором возможностей для мониторинга сетевой активности, анализа трафика, обнаружений аномалий [1].

Коммерческие решения остаются недоступными для многих небольших компаний из-за высокой стоимости лицензий, сложности внедрения и требований к квалификации персонала.

Результаты исследования позволяют с уверенностью утверждать, что система Arkime может конкурировать с коммерческими продуктами для специфических задач, предоставляя мощные инструменты для мониторинга и исследования сетевых инцидентов. Arkime является наиболее подходящим для создания универсальной системы ретроспективного анализа, так как представляет собой комплекс множества инструментов, распространяемых по свободной лицензии [2, с. 60].

По совокупности критериев Arkime имеет ряд достоинств: открытый исходный код, поддержка некоммерческого использования, наличие возможности воспроизведения трафика и анализа прикладных протоколов, а также полнотекстового поиска по пакетам и интеграции с внешними источниками угроз. Arkime является представителем класса систем NTA (Network Traffic Analysis), которые предназначены для глубокого пассивного мониторинга, анализа, сбора и индексации всего сетевого трафика в режиме реального времени. Как правило, анализаторы сетевого трафика имеют модульную структуру. Это обусловлено тем, что со временем появляются новые протоколы, и их необходимо поддерживать [3]. Такой подход обеспечивает долгосрочную поддержку разнообразных технологий и адаптивность Arkime к эволюции сетевой среды.

Для обнаружения компьютерных атак в основном используются сигнатурные анализаторы сетевого трафика, эффективность которых ограничена полнотой базы решающих правил обнаружения известных информационных воздействий [4]. В отличие от них, платформа Arkime реализует подход, основанный на полном захвате трафика и ретроспективном анализе, позволяя находить скрытые индикаторы компрометации в отсутствие заранее известных сигнатур.

В работе проведено экспериментальное исследование: развернута тестовая среда, реализован сбор и анализ трафика с использованием методов DPI (Deep Packet Inspection-глубокая инспекция пакетов) и метаданных, протестированы сценарии обнаружения, включая C2-активность, сигнатурный анализ и интеграцию с внешними источниками угроз.

Глубокий анализ пакетов (DPI) – классический метод классификации трафика, который фокусируется на полезной нагрузке [5]. При помощи DPI решаются такие задачи, как выделение групп пользователей по трафику, выделение приложений, а также отдельных функций приложений [6].

В рамках исследования были проверены следующие функциональные возможности платформы Arkime: анализ захваченного трафика (PCAP-анализ), выявление известных угроз на основе индикаторов компрометации из готовых файлов трафика, настройка информационных дашбордов, обнаружение атак типа Command Control (C2), проверка файлов через интеграцию с VirusTotal, поиск сессий по заданным метаданным.

Цель исследования – оценить возможности платформы с открытым исходным кодом Arkime для обнаружения и расследования сетевых атак.

Материалы и методы исследования

В ходе исследования была развернута тестовая лаборатория на базе операционной системы Ubuntu с установленной платформой Arkime и целевыми системами Windows 11 и Windows Server 2008. Для сбора и анализа данных использовались методы глубокого анализа пакетов и метаданных. Методы, основанные на анализе сетевого трафика, позволяют выявлять атаки в режиме реального времени, анализируя заголовки и содержимое сетевых пакетов [7, с. 56]. Полноценное расследование инцидентов невозможно без централизованного сбора, хранения и индексации сетевых данных, включая PCAP-файлы [8]. Для эмуляции атак используем заранее записанные PCAP-файлы, воспроизводимые в сеть с помощью утилиты tcpreplay. Трафик доставляется на целевые системы, а сенсор Arkime на Ubuntu пассивно захватывает его через виртуальный интерфейс типа VMXNET3, настроенный на использование режима AF_PACKET, что является необходимым условием для эффективного захвата сетевых пакетов. Arkime индексирует пакеты, извлекает сессии, файлы и метаданные, обеспечивая основу для ретроспективного расследования. Тестирование включает восстановление атак по PCAP-файлам, проверку обнаружения вредоносного программного обеспечения и оценку эффективности инструментов мониторинга в сценариях, приближенных к реальным. Использованы инструменты глубокой проверки пакетов DPI – обеспечивают стопроцентную прозрачность сети, преобразуя необработанные метаданные в читаемый формат [9]. В DPI, помимо изучения заголовков пакетов, все содержимое каждого пакета сравнивается с набором сигнатур, чтобы проверить, не обнаружена ли какая-либо сигнатура в пакете [10].

Алгоритмы тестирования и математическая модель анализа

Для формализации процесса анализа представим работу платформы Arkime как систему преобразования сетевого трафика в структурированное пространство признаков. Сетевой трафик представим как временной ряд пакетов:

$$T = \{p_1, p_2, \ldots, p_n\},$$

где каждый пакет p_i характеризуется набором атрибутов:

$$p_i = (\text{src\_ip},\ \text{dst\_ip},\ \text{dst\_port},\ \text{protocol}, \text{timestamp}, \text{payload}),$$

что определяет его положение в многомерном пространстве. Здесь src_ip, dst_ip – IP-адреса источника и назначения соответственно, dst_port – порт назначения, protocol – тип протокола, timestamp – время захвата пакета, payload – полезная нагрузка (полезные данные, которые передаются) в сети.

Алгоритм платформы Arkime выполняет следующие ключевые преобразования:

1. Группировка пакетов в сессии (соединения): Сессия s_j определяется как множество пакетов, связанных одинаковой четверкой параметров:

$$s_j = \left\{\left(\text{src}_{ip},\ \text{dst}_{ip},\ \text{src}_{potr},\ \text{dst}_{port}\right)\right\} \subseteq T.$$

Это эквивалентно разбиению множества T на непересекающиеся подмножества по отношению эквивалентности.

2. Извлечение признаков и построение векторного описания. Для каждой сессии вычисляются числовые и категориальные признаки: длительность Δt, количество пакетов N_p, объем передаваемых данных V (в байтах), тип протокола прикладного уровня (HTTP, DNS, SMB и др.), наличие сигнатур из базы Emerging Threats. Эти признаки образуют вектор

$$\vec{x}_j = (x_1, x_2, \ldots x_k),$$

который используется для последующей классификации и поиска аномалий.

3. Обнаружение угроз как задача бинарной классификации. Процесс детектирования может быть сформулирован как функция решения

$$f(\vec{x}_j) \to \{0,1\},$$

где f – правило, основанное на наличии индикаторов компрометации.

В случае сигнатурного анализа используется детерминированная функция:

$$f_{rule}(x) = \begin{cases} 1, \text{если } \exists \text{ строка } s \in payload,\ s \in S_{indicators} \\ 0, \text{ иначе,} \end{cases},$$

где $S_{indicators}$ – множество индикаторов компрометации.

4. Хеширование и идентификация объектов. Файлы, извлекаемые из трафика, отображаются в однозначный цифровой идентификатор – хэш. При использовании VirusTotal это реализуется как отображение:

$$h = H(data),$$

$$H \in \{MD5, SHA-1, SH-256\}.$$

Таким образом, платформа Arkime функционирует не только как программный комплекс, но и как система, реализующая математические модели обработки данных.

Результаты исследования и их обсуждение

После запуска системы начинается захват трафика, который становится доступен для просмотра в веб-интерфейсе Arkime.

Обнаружение угроз в сетевом дампе

Для анализа угроз использовался заранее записанный файл трафика signatures.pcap, загруженный в Arkime. Платформа индексирует трафик, извлекает файлы и выявляет известные индикаторы компрометации. Для эмуляции атаки в лабораторной среде использована утилита tcpreplay. Для эмуляции трафика командой *sudo tcpreplay –M 10 –I ens 192 signatures.pcap*. производится воспроизведение пакетов из файла signatures.pcap через сетевой интерфейс ens192 на скорости, в 10 раз превышающей скорости захвата. Полученные сигнатурные инциденты представлены на рис. 1.

Система осуществила глубокий анализ сетевого трафика, включая типы протоколов, IP-адреса отправителя и получателя, используемые порты, длительность сеансов и содержимое заголовков сетевых протоколов (только для незашифрованных протоколов). При воспроизведении трафика из файла signatures.pcap, система зафиксировала 82 события, включая сканирование портов с помощью nmap, эксплуатацию уязвимостей и передачу вредоносных файлов (рис. 1).

+	tcp	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)	2024/06/03 04:11:26	2024/06/03 04:11:26	10.1.75.4	63932	42.115.91.177	443	20	2,206 3,302	ubuntu22		
+	tcp	ET MALWARE W32/Emotet CnC Checkin	2024/06/03 04:11:26	2024/06/03 04:11:26	10.1.75.167	62394	87.66.13.80	80	759	610,654 651,656	ubuntu22	URI ▾	87.66.13.80/
+	tcp	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)	2024/06/03 04:11:26	2024/06/03 04:11:26	10.1.75.167	62393	31.179.162.86	443	24	2,659 3,971	ubuntu22		
+	tcp	ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010 ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	2024/06/03 04:11:26	2024/06/03 04:11:26	10.1.75.167	62349	10.1.75.4	445	86	67,643 72,311	ubuntu22		
+	tcp	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)	2024/06/03 04:11:26	2024/06/03 04:11:26	10.1.75.167	62345	31.179.162.86	443	53	6,862 9,740	ubuntu22		
+	tcp	ET POLICY PE EXE or DLL Windows file download HTTP ET INFO Packed Executable Download ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response ET USER_AGENTS Suspicious User-Agent (contains loader)	2024/06/03 04:11:25	2024/06/03 04:11:26	10.1.75.4	63620	192.161.54.60	80	850	785,677 831,595	ubuntu22	URI ▾	192.161.54.60/radianc 192.161.54.60/table.png
+	tcp	ET MALWARE Trickbot Checkin Response	2024/06/03 04:11:25	2024/06/03 04:11:25	10.1.75.4	63618	200.29.24.36	8082	13	690 1,408	ubuntu22	URI ▾	200.29.24.36:8082/lib322/PIX E-DC_W617601.EB82F8C32F E749EF8128735E0F5/81/

Рис. 1. Список обнаруженных сетевых инцидентов в файле signatures.pcap
Примечание: составлен авторами по результатам данного исследования

Рис. 2. Сетевая активность, связанная с выполнением команд злоумышленником
Примечание: составлен авторами по результатам данного исследования

На скриншоте представлен перечень угроз, включающий соединение с ботнетом Emotet, попытку эксплуатации уязвимости EternalBlue, загрузку исполняемого файла, подозрительный ответ от хоста и аномальный User-Agent.

Анализ C2-активности

Анализ статистических и временных характеристик сетевого трафика позволяет выявлять аномалии, связанные с C2-коммуникациями и эксфильтрацией данных. Arkime позволяет выявлять атаки, использующие технику команд и управления (C2), путем анализа сетевых сессий на наличие характерных шаблонов, таких как ключевые слова DownloadFile, SharpSploit.dll и других типовых индикаторов C2-активности.

Не каждая аномалия в сетевом трафике представляет собой угрозу информационной безопасности. Для повышения точности определения неправомерных действий внутри защищенного периметра сети необходимо учитывать множество факторов: источники и причины сетевых аномалий, количество аномалий и их потенциальную связь между собой [11, с. 46].

В тестовой среде моделировалось C2-взаимодействие, которое представляет собой контролируемую имитацию подключения, компрометирующего ПО к командному серверу, воспроизводящую типичное поведение реальных вредоносных программ для целей анализа и обнаружения. В демонстрационном сценарии воспроизводится сетевая активность для C2-взаимодействия, нацеленного на контроллер домена. Для этого с помощью утилиты *tcpreplay* в сеть отправляется заранее записанный трафик sharpsploit_cnc.pcap, имитирующий обращение компрометированной системы к удаленному серверу управления. Воспроизведенный сценарий соответствует типичной цепочке атаки: получение жертвой фишингового письма, переход по вредоносной ссылке, загрузка вредоносного программного обеспечения и установления C2-канала. Представленный ниже пример демонстрирует имитацию атаки, направленной на контроллер домена, с последующим обнаружением подозрительной активности средствами Arkime.

Для тестирования систем обнаружения вторжений часто используется метод воспроизведения реального сетевого трафика с помощью инструментов, таких как tcpreplay, которые позволяют инжектировать ранее захваченные PCAP-файлы в сеть с заданной скоростью и через указанный сетевой интерфейс, что обеспечивает воспроизводимость экспериментальных условий и точное моделирование [12, с. 363–364].

Симуляцию сетевой активности атаки осуществим путем воспроизведения записанного трафика с помощью утилиты

tcpreplay: sudo tcpreplay -M 10 -i ens192 sharpsploit_cnc.pcap,

где *M* задает скорость воспроизведения – 10 Mbps, а *ens192* – сетевой интерфейс, через который передается трафик.

На рис. 2 отображается детализованный анализ сетевой сессии, в которой обнаружены признаки атаки, связанные с использованием банковского трояна TrickBot. В верхней части представлен список сигнатур безопасности от Emerging Threats (ET), отнесенных к категории HUNTING, что указывает на целенаправленное выявление скрытых и малоизвестных угроз. Видны IP-адреса источника и назначения, временные метки, порты, объем захваченного трафика и детали HTTP-запросов, включая тело сообщения, где содержится сам код команд. Сигнатуры ET HUNTING пометили трафик как связанный с банковским трояном TrickBot, используемый для кражи данных.

Данный пример иллюстрирует, как инструменты класса NTA способны обеспечить видимость действий злоумышленника на этапе установления контроля над компрометированной системой.

Визуализация сетевых событий с помощью дашборда

Для упрощения анализа сетевого трафика специалист информационной безопасности может использовать визуализацию данных через вкладку SPIGraph в интерфейсе Arkime. Среди миллионов сессий бывает сложно вовремя заметить аномалии или получить целостное представление о происходящем в сети. SPIGraph предоставляет наглядную иерархическую визуализацию сетевых событий, что позволяет быстро выявлять наиболее активные категории угроз и оперативно реагировать на инциденты. В рамках тестового сценария применим фильтры для отбора релевантных сессий и проанализируем структуру событий (рис. 3).

Диаграмма представляет собой солнечный график, где внутренние кольца отражают общие категории инцидентов, а внешние – их детализацию до уровня конкретных сигнатур. Система зафиксировала 82 события, соответствующих сигнатуре ET SCAN Possible Nmap User-Agent, что указывает использование инструмента nmap для сетевого сканирования.

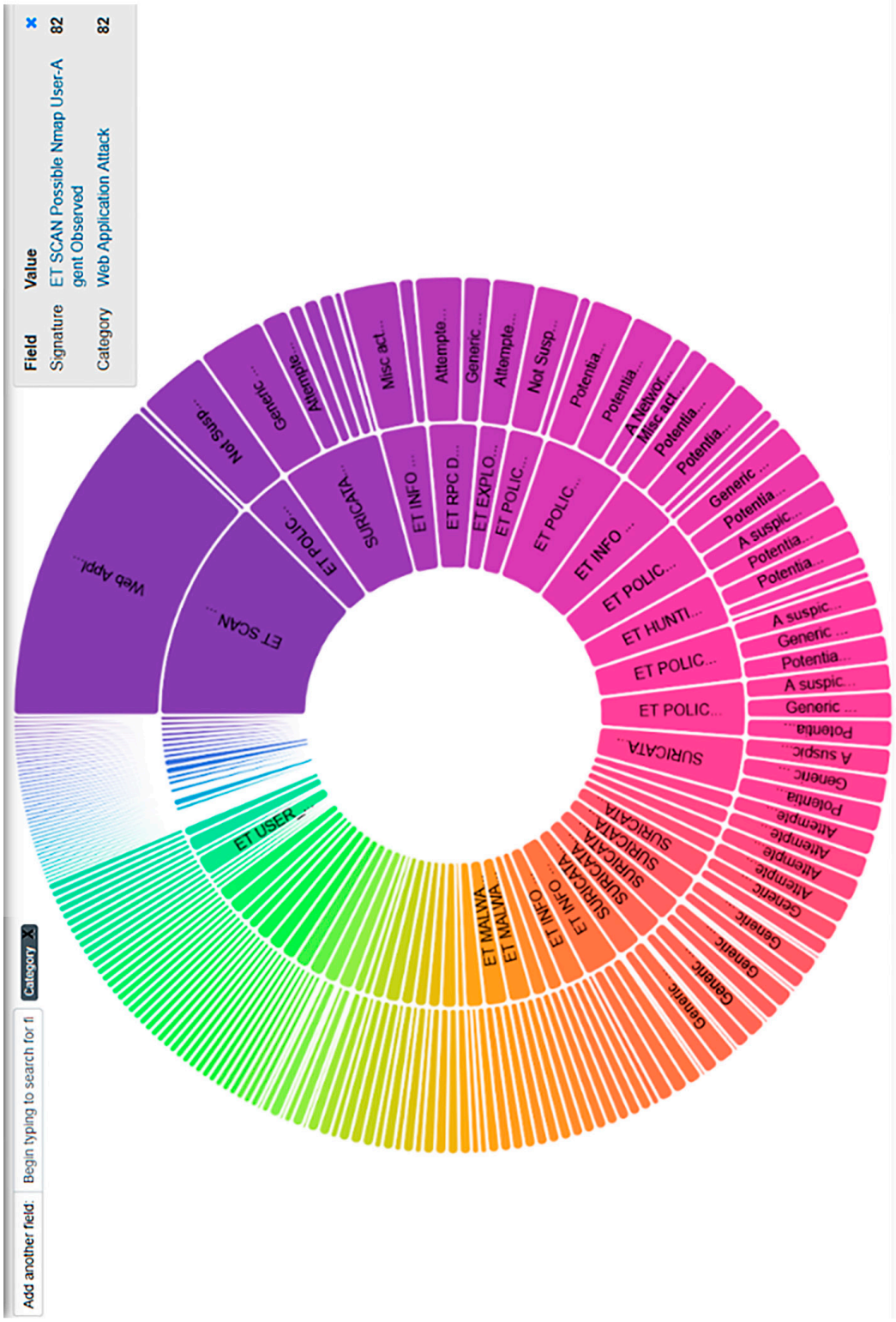

Рис. 3. Визуализация дашборда: сетевые события
Примечание: составлен авторами по результатам данного исследования

Помимо сканирования диаграмма выявляет наличие событий, относящихся к категориям: эксплуатация уязвимости, вредоносное программное обеспечение и атаки на веб-приложения, что свидетельствует о комплексном характере атаки, включающем как разведку, так и попытки компрометации. Такая визуализация позволяет быстро оценить распределение угроз и определить наиболее активные векторы атаки.

Сценарий интеграции Arkime с VirusTotal для обнаружения вредоносных загрузок

Проверка файлов через Virus Total осуществляется путем извлечения их хэш-суммы из сетевого трафика и последующего сопоставления с антивирусными базами.

Современные платформы (например, Moloch, ныне Arkime) способны автоматически извлекать файлы из протоколов HTTP, FTP и других протоколов, вычислять их хэш-суммы (MD5, SHA1, SHA256) и сохранять их в индексированной базе. Эти хэши позволяют мгновенно составлять объекты с внешними источниками угроз, такими как VirusTotal, ReversingLabs или внутренние репутационные базы, что является ключевым компонентом расследования инцидентов, связанного с вредоносными загрузками [13].

Основное внимание в данном сценарии уделяется мониторингу передачи файлов и использованию хэшей для быстрой идентификации потенциально опасного контента.

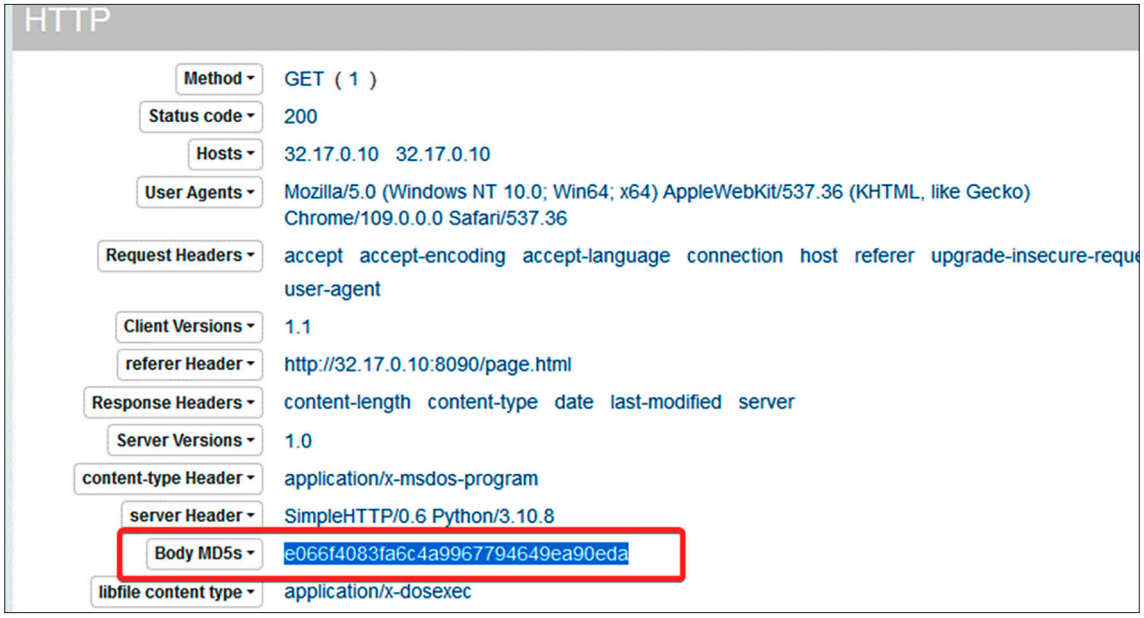

Рис. 4. Разбор инцидента
Примечание: составлен авторами по результатам данного исследования

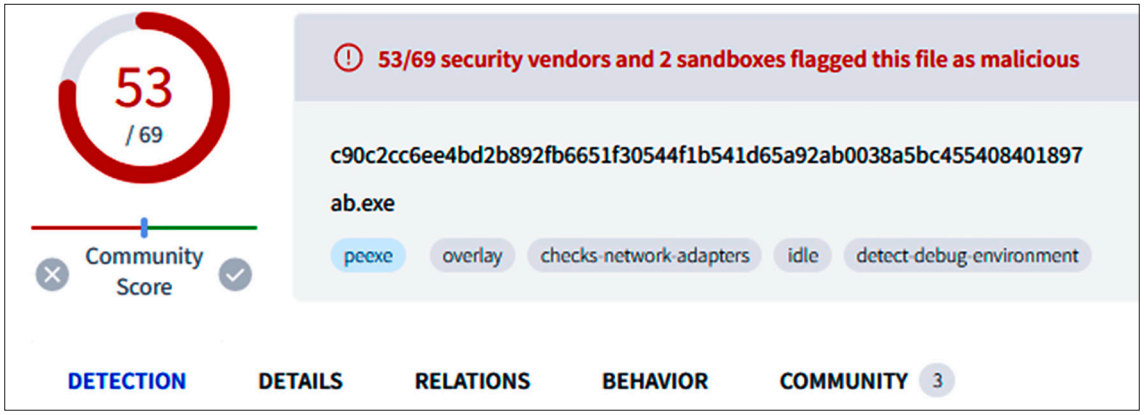

Рис. 5. Отчет антивирусного сканирования файла
Примечание: составлен авторами по результатам данного исследования

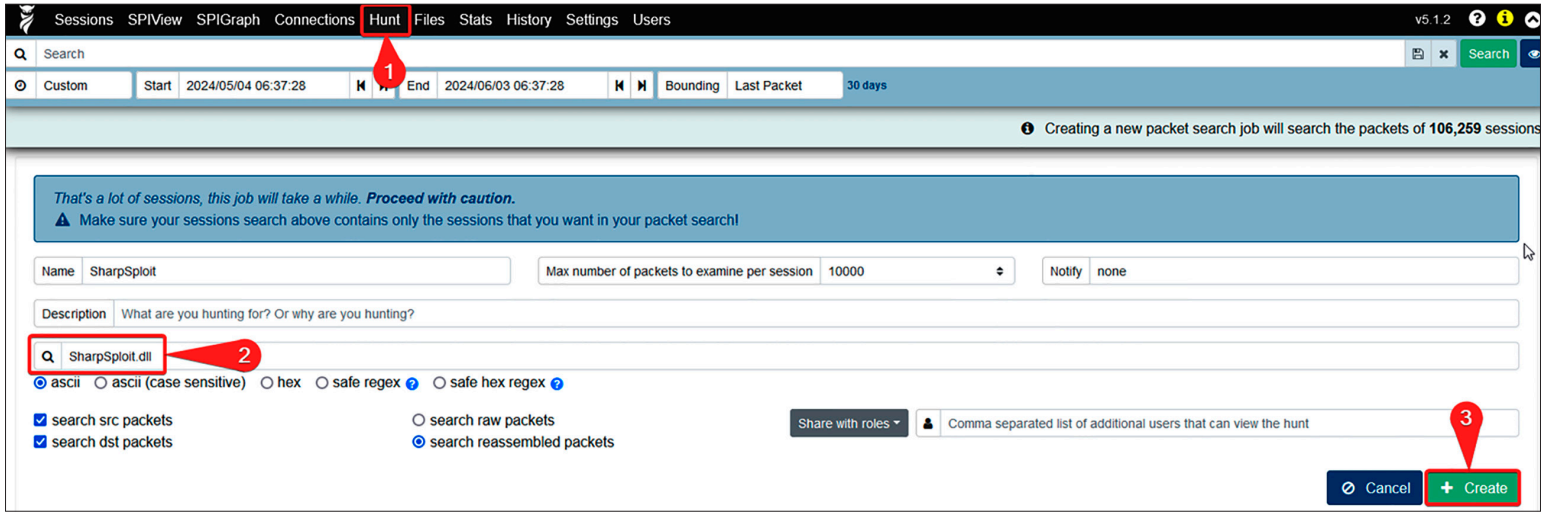

Рис. 6. Модуль Hunt: создание поисковой задачи для выявления сессий, содержащих строку SharpSploit.dll
Примечание: составлен авторами по результатам данного исследования

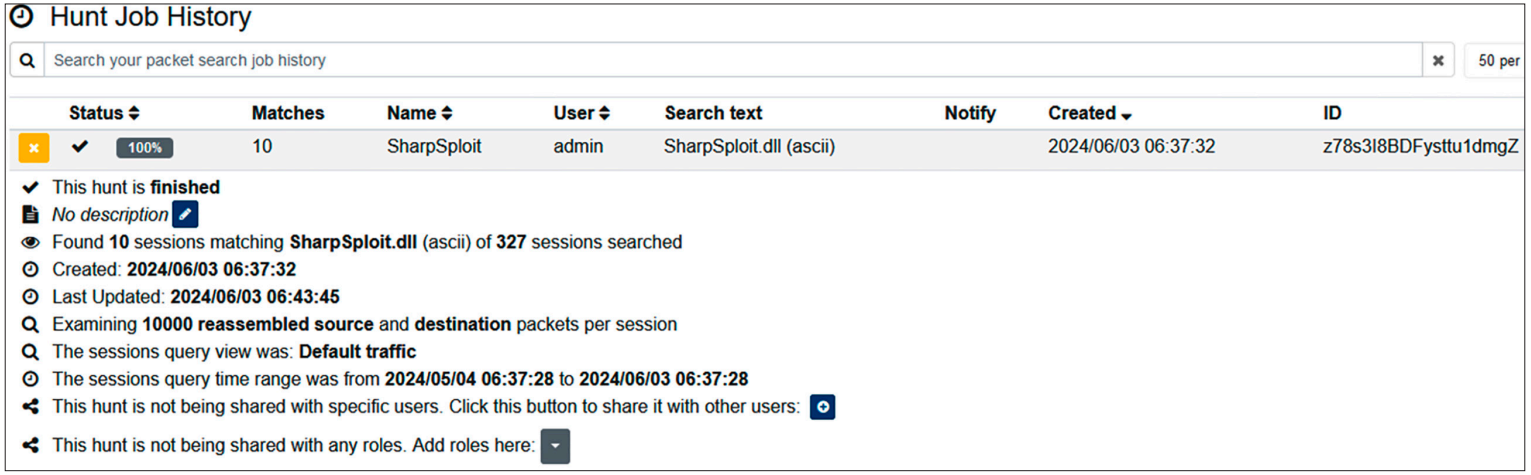

Рис. 7. Визуализация результата поиска по строке SharpSploit.dll
Примечание: составлен авторами по результатам данного исследования

huntid == z78s3l8BDFystlu1dmg2

Custom | Start | 2024/05/04 06:37:28 | End | 2024/06/03 06:37:28 | Bounding | Last Packet | Interval | Auto | 30 days | Search | Fetch Viz Data

50 per page | 1 | Showing 1 - 10 of 10 entries

This cluster is set to hide the graph if a time range of 30 days or greater is requested
Click the "Fetch Viz Data" button above to fetch visualization data for this query (or open the dropdown for more options).

	Signature	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Arkime Node	Info
tcp	ET INFO Dotted Quad Host DLL Request ET MALWARE Mimikatz x86 Executable Download Over HTTP ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download ET POLICY PE EXE or DLL Windows file download HTTP ET MALWARE Mimikatz x64 Executable Download Over HTTP	2024/06/03 04:11:02	2024/06/03 04:11:04	192.168.202.102	53542	45.92.208.33	8080	1,789	2,222,884 2,319,526	ubuntu22	URI 192.168.202.145:8080/Sharpl
tcp	ET POLICY Command Shell Activity Using Comspec Environmental Variable Over SMB - Very Likely Lateral Movement ET POLICY Powershell Activity Over SMB - Likely Lateral Movement	2024/06/03 04:11:02	2024/06/03 04:11:05	192.168.202.101	54908	192.168.202.102	445	246	43,870 57,178	ubuntu22	
tcp	ET INFO Dotted Quad Host DLL Request ET MALWARE Mimikatz x86 Executable Download Over HTTP ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download ET POLICY PE EXE or DLL Windows file download HTTP ET MALWARE Mimikatz x64 Executable Download Over HTTP	2024/06/03 00:36:38	2024/06/03 00:36:40	192.168.202.102	53542	45.92.208.33	8080	1,789	2,222,884 2,319,526	ubuntu22	URI 192.168.202.145:8080/Sharpl
tcp	ET POLICY Command Shell Activity Using Comspec Environmental Variable Over SMB - Very Likely Lateral Movement ET POLICY Powershell Activity Over SMB - Likely Lateral Movement	2024/06/03 00:36:38	2024/06/03 00:36:40	192.168.202.101	54908	192.168.202.102	445	246	43,870 57,178	ubuntu22	
tcp	ET POLICY PE EXE or DLL Windows file download HTTP ET MALWARE Mimikatz x64 Executable Download Over HTTP ET INFO Dotted Quad Host DLL Request ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download ET MALWARE Mimikatz x86 Executable Download Over HTTP	2024/05/18 06:05:57	2024/05/18 06:05:59	192.168.202.102	53542	45.92.208.33	8080	1,789	2,222,884 2,319,526	ubuntu22	URI 192.168.202.145:8080/Sharpl
tcp	ET POLICY Powershell Activity Over SMB - Likely Lateral Movement ET POLICY Command Shell Activity Using Comspec Environmental Variable Over SMB - Very Likely Lateral Movement	2024/05/18 06:05:57	2024/05/18 06:05:59	192.168.202.101	54908	192.168.202.102	445	246	43,870 57,178	ubuntu22	
tcp	ET POLICY PE EXE or DLL Windows file download HTTP ET MALWARE Mimikatz x64 Executable Download Over HTTP ET INFO Dotted Quad Host DLL Request ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download ET MALWARE Mimikatz x86 Executable Download Over HTTP	2024/05/18 06:04:19	2024/05/18 06:04:21	192.168.202.102	53542	45.92.208.33	8080	1,789	2,222,884 2,319,526	ubuntu22	URI 192.168.202.145:8080/Sharpl
tcp	ET POLICY Powershell Activity Over SMB - Likely Lateral Movement ET POLICY Command Shell Activity Using Comspec Environmental Variable Over SMB - Very Likely Lateral Movement	2024/05/18 06:04:19	2024/05/18 06:04:22	192.168.202.101	54908	192.168.202.102	445	246	43,870 57,178	ubuntu22	
tcp	ET POLICY PE EXE or DLL Windows file download HTTP ET MALWARE Mimikatz x64 Executable Download Over HTTP ET INFO Dotted Quad Host DLL Request ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download ET MALWARE Mimikatz x86 Executable Download Over HTTP	2024/05/18 06:01:11	2024/05/18 06:01:13	192.168.202.102	53542	45.92.208.33	8080	1,789	2,222,884 2,319,526	ubuntu22	URI 192.168.202.145:8080/Sharpl
tcp	ET POLICY Powershell Activity Over SMB - Likely Lateral Movement ET POLICY Command Shell Activity Using Comspec Environmental Variable Over SMB - Very Likely Lateral Movement	2024/05/18 06:01:11	2024/05/18 06:01:13	192.168.202.101	54908	192.168.202.102	445	246	43,870 57,178	ubuntu22	

Рис. 8. Анализ сетевого трафика

Примечание: составлен авторами по результатам данного исследования

Для безопасного тестирования средств обнаружения вторжений рекомендуется использовать стандартный тестовый файл EICAR, размещенный на официальном сайте eicar.org, который распознается всеми антивирусными продуктами как сигнатура вредоносной программы, не выполняя при этом вредоносных действий. Воспользуемся этим файлом для исследования. Эмуляция атаки выполняется командой: *curl –LO https://secure.eicar.org/eicar.com && ls -lah*

В карточке HTTP-сессии в Arkime копирует MD5-хэш файла eicar.com. Хэш файла копируется из интерфейса Arkime и вручную проверяется на сайте VirusTotal для получения вердикта от антивирусных движков.

На рис. 4 представлен анализ HTTP-запроса, в котором видно, что сервер 32.17.0.10:8080 вернул файл с MIME-типом *application/x-msdos-program*, что соответствует исполняемому файлу для Windows. Arkime автоматически извлекает тело ответа и вычисляет его MD5-хэш-значение. Этот хэш может быть использован для проверки файла на вредоносность вне зависимости от его имени и расширения, что особенно важно при анализе скрытых или обфусцированных загрузчиков.

Анализ реального вредоносного файла в трафике

Результаты антивирусного сканирования файла *ab.exe* с использованием сервиса VirusTotal представлены на рис. 5.

Из 69 антивирусных движков 53 идентифицировали этот файл как вредоносный, что подтверждает корректность механизма хэширования и интеграции. Анализ поведения файла указывает на потенциально вредоносные действия: проверка сетевых и попытка обнаружения среды отладки, что характерно для malware, стремящегося скрыть свое присутствие и оценить окружение.

Поиск сессий по метаданным и содержимому пакетов

Arkime предоставляет модуль Hunt, предназначенный для выполнения глубокого поиска по содержимому сетевых пакетов, включая данные полезной нагрузки, что позволяет обнаруживать признаки вредоносного программного обеспечения, даже если они скрыты в кодировке Base64 (рис. 6).

Для расследования создается задача Hunt в Arkime с поиском строки SharpSploit.dll, после выполнения которой в результатах отображаются все сессии, содержащие указанную строку (рис. 7). По запросу SharpSploit.dll было проанализировано 527 сессий, из которых 10 содержали указанную строку, что свидетельствует о наличии активности в сетевом трафике, связанной с использованием фреймворка SharpSploit-инструмента, который часто используется злоумышленниками для выполнения кода, сбора данных и перемещения по сети. Файл SharpSploit.dll может быть связан с атаками, такими как DLL Hijacking или эксплуатация уязвимостей, в том числе в Microsoft Share Point.

На рис. 8 представлен список сетевых сессий, в которых обнаружены сигнатуры безопасности, указывающие на подозрительную или вредоносную активность.

Сигнатуры указывают на действия, характерные для вредоносного программного обеспечения [14; 15]. Они являются индикаторами компрометации. В частности, можем выделить сигнатуры ETPOLICY Command Shell Activity и ETPOLICY Command Shell Activity и ETINFO Executable Download Over HTTP, которые свидетельствуют о выполнении командной оболочки через сетевые протоколы и о загрузке исполняемых файлов по HTTP. Наличие таких сигнатур указывает на высокую вероятность компрометации системы.

Заключение

Экспериментальное исследование подтвердило, что платформа Arkime обладает функциональностью, соответствующей задачам системы класса NTA. В ходе эксперимента Arkime осуществлял захват и анализ сетевого трафика в режиме, имитирующем реальное время, при воспроизведении заранее записанных атак с помощью утилиты tcpreplay. Были успешно продемонстрированы ее ключевые возможности: захват и декодирование сетевого трафика, автоматическое извлечение передаваемых файлов и вычисление хэш-сумм, выявление известных угроз на основе анализа индикаторов компрометации из готовых дампов трафика, обнаружение аномальной активности, характерной для C2-взаимодействия, идентификации передачи вредоносных файлов и их проверка через интеграцию VirusTotal, а также поиск сессий по заданным строкам с использованием модуля Hunt и визуализация сетевых событий через настраиваемые дашборды и интерактивную карту взаимодействия.

Платформа Arkime предоставляет администраторам и аналитикам средства для оперативного обнаружения угроз, расследования инцидентов и выполнения базовых требований информационной безопасности. Благодаря открытому исходному коду и низким аппаратным требованиям, Arkime представляет собой экономически обоснованную альтернативу коммерческим NTA-решениям, особенно для организаций

с ограниченным бюджетом. Его внедрение позволит расширить возможности сетевого мониторинга и повысить защищенность информационной инфраструктуры без значительных финансовых затрат.

Список литературы

1. Власова А. В., Дударев В. А., Новикова Т. И. Сравнительный анализ open-source инструментов мониторинга информационной безопасности // Сборник научных статей по материалам IX Международной научно-практической конференции (г. Уфа, 02 декабря 2022 г.). Ч. 2. Уфа: Вестник науки, 2022. С. 164–174. [Электронный ресурс]. URL: https://www.elibrary.ru/item.asp?id=49927440 (дата обращения: 15.11.2025).

2. Пырьев М. С., Коллеров А. С. Средства анализа сетевого трафика локальной вычислительной сети в ретроспективе // Вестник УрФО. Безопасность в информационной сфере. 2019. № 4 (34). С. 58–62. URL: https://elibrary.ru/item.asp?id=41879988 (дата обращения: 15.11.2025).

3. Гетьман А. И., Иванников В. П., Маркин Ю. В., Падарян В. А., Тихонов А. Ю. Модель представления данных при проведении глубокого анализа сетевого трафика // Труды Института системного программирования РАН. 2015. № 27 (4). С. 5–22. DOI: 10.15514/ISPRAS-2015-27(4)-1.

4. Гетьман А. И., Горюнов М. Н., Мацкевич А. Г., Рыболовлев Д. А. Методика сбора обучающего набора данных для модели обнаружения компьютерных атак // Труды Института системного программирования РАН. 2021. № 33 (5). С. 83–104. DOI: 10.15514/ISPRAS-2021-33(5)-5.

5. Macas M., Wu C., Fuertes W. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities // Computer Networks. 2022. Vol. 212. P. 109032. DOI: 10.1016/j.comnet.2022.109032.

6. Пономаренко Р. Е., Егоров В. И., Гетьман А. И. Вызовы в реализации систем глубокого анализа сетевого трафика методом полного протокольного декодирования // Труды Института системного программирования РАН. 2023. Т. 35. № 4. С. 45–64. URL: https://www.elibrary.ru/item.asp?id=59762177 (дата обращения: 19.11.2025).

7. Фролов П. В., Вершинин Е. В., Медведева С. А. Исследование методов обнаружения сетевых атак // Вопросы радиоэлектроники. 2019. № 11. С. 55–59. URL: https://elpub.ru/elpub-article/vopradio/1060 (дата обращения: 21.11.2025). DOI: 10.21778/2218-5453-2019-11-55-59.

8. Сандерс К. Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях. 3-е изд. / Пер. с англ. СПб.: ООО «Диалектика», 2019. 448 с. [Электронный ресурс]. URL: https://psv4.userapi.com/s/v1/d/Cgdtzgul9vqaVrrR4Dx9piLttQVd162RW6IgjkEpYyB1sW0EZKKPDzCNnt9KB8oIBMt9BkErIyIikNRUKX2YAVmz0cstV24p_vhur0Ac3KJ8vNmH/Sanders_K_Analiz_paketov_3_e_izdanie.pdf (дата обращения: 21.11.2025). ISBN 978-5-6040723-0-1.

9. Тураев С. Э., Заколдаев Д. А. Анализ сетевого трафика (АСТ) в кибербезопасности // Наука и бизнес: пути развития. 2024. № 5 (155). С. 61–65. URL: https://elibrary.ru/item.asp?id=69159305 (дата обращения: 21.11.2025).

10. Беленькая М. Н., Зайцев Е. С., Акопян В. А., Кошепаров Д. Я. Обзор методов анализа сетевого трафика средствами DPI // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2018. № 1. С. 15–20. URL: https://elibrary.ru/item.asp?id=37062191 (дата обращения: 22.11.2025).

11. Будько М. Б., Малько А. Д., Стародубова Д. Д., Стародубов Р. Д. Обнаружение аномалий сетевого трафика: основные аспекты, проблемы и методы // Современная наука: актуальные проблемы теории и практики. Серия: естественные и технические науки. 2020. № 8. [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=44027319 (дата обращения: 25.11.2025). DOI: 10.37882/2223-2966.2020.08.05.

12. Shiravi A., Shiravi H., Tavallaee M., Ghorbani A. A. Toward Developing a Systematic Approach to Generate Benchmark Datasets for Intrusion Detection@//Computers & Security, 2012. Vol. 31. Is. 3. P. 357–374. URL: https://www.researchgate.net/publication/257006500_Toward_developing_a_systematic_approach_to_generate_benchmark_datasets_for_intrusion_detection. (дата обращения: 01.12.2025). DOI: 10.1016/j.cose.2011.12.012.

13. Chuvakin A., Schmidt K., Phillips C. (2012). Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. URL: https://www.researchgate.net/publication/294592364_Logging_and_Log_Management_The_Authoritative_Guide_to_Understanding_the_Concepts_Surrounding_Logging_and_Log_Management (дата обращения: 01.12.2025).

14. Mathur Lakshya, Raheja Mayank, Chaudhary Prachi. Botnet Detection via mining of network traffic flow // Procedia Computer Science. 2018. Vol. 132. P. 1668–1677. URL: https://www.researchgate.net/publication/325657302_Botnet_Detection_via_mining_of_network_traffic_flow (дата обращения: 11.03.2026). DOI: 10.1016/j.procs.2018.05.137.

15. Ларин Д. В., Гетьман А. И. Средства захвата и обработки высокоскоростного сетевого трафика // Труды Института системного программирования РАН. 2021. № 33 (4). С. 49–68. DOI: 10.15514/ISPRAS-2021-33(4)-4.

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest: The authors declare that there is no conflict of interest.