УДК 004.738.5

АНАЛИЗ УГРОЗ ПЕРЕХВАТА ТРАФИКА И ЭФФЕКТИВНЫЕ МЕТОДЫ ЗАЩИТЫ

Исрафилов А.

магистр, индивидуальный исследователь

Дроздов И.С.

бакалавр,

Московский государственный технический университет им Н.Э. Баумана,

Москва, Россия

Письменский Д.А.

бакалавр,

Московский государственный технический университет им Н.Э. Баумана,

Москва, Россия

Аннотация

В современном мире, где значительная часть жизнедеятельности человека переместилась в цифровое пространство, вопросы кибербезопасности обретают всё большее значение. Одной из ключевых угроз в этом контексте является перехват трафика, который может включать в себя как пассивные методы наблюдения за данными пользователя без их изменения, так и активные атаки с целью перехвата, модификации или перенаправления цифровых потоков. По статистике, активные и пассивные методы перехвата трафика составляют значительную долю инцидентов в области кибербезопасности, что усиливает потребность в разработке и внедрении комплексных систем защиты. Особое внимание в статье уделено изучению различных подходов к обеспечению информационной безопасности, включая шифрование данных по протоколам SSL/TLS, использование HTTPS в целях снижения рисков Man-in-the-Middle

атак, применение end-to-end шифрования для гарантии конфиденциальности пересылаемой информации, многофакторную аутентификацию как средство повышения надёжности проверки подлинности пользователей, а также использование систем обнаружения и предотвращения вторжений, способных своевременно реагировать на попытки несанкционированного доступа. В статье подчёркивается, что ни один метод защиты не является абсолютно надёжным в изоляции, и истинная безопасность достижима только путём интеграции различных инструментов и подходов. Анализируется взаимодополняемость методов шифрования, многофакторной аутентификации и систем мониторинга сети, что иллюстрируется статистикой успешности противостояния киберугрозам. В заключение акцентируется важность адаптивности и гибкости стратегий кибербезопасности для эффективного реагирования на постоянно изменяющиеся киберугрозы, подкрепляя это аргументацией о необходимости широкого внедрения комплексных решений на всех уровнях информационной инфраструктуры предприятий и организаций. Таким образом, статья предлагает фундаментальный анализ угроз перехвата трафика и обзор повсеместных методов их предотвращения, подчёркивая стратегическую важность комплексного подхода к обеспечению кибербезопасности в условиях непрерывно эволюционирующего цифрового пространства.

Ключевые слова: кибербезопасность, перехват трафика, шифрование данных, многофакторная аутентификация, системы обнаружения и предотвращения вторжений.

ANALYSIS OF TRAFFIC INTERCEPTION THREATS AND EFFECTIVE PROTECTION METHODS

Israfilov A.

master's degree, individual researcher

Drozdov I.S.
bachelor's degree,
Bauman Moscow State Technical University,
Moscow, Russia

Pismenskiy D.A.
bachelor's degree,
Bauman Moscow State Technical University,
Moscow, Russia

Abstract

In the contemporary world, where a significant portion of human activity has shifted into the digital space, cybersecurity issues have increasingly gained prominence. A key threat in this context is traffic interception, which may involve both passive methods of monitoring user data without altering it and active attacks aimed at interception, modification, or redirection of digital flows. Statistics show that active and passive traffic interception methods constitute a significant proportion of incidents in the realm of cybersecurity, thereby amplifying the need for the development and implementation of comprehensive protection systems. This paper pays special attention to the study of various approaches to ensuring information security, including data encryption via SSL/TLS protocols, the use of HTTPS to reduce the risks of Man-in-the-Middle attacks, the application of end-to-end encryption to guarantee the confidentiality of transmitted information, multifactor authentication as a means to enhance the reliability of user authentication, and the utilization of intrusion detection and prevention systems capable of timely responding to unauthorized access attempts. The article emphasizes that no single protection method is absolutely reliable in isolation, and true security is achievable only through the integration of various tools and approaches. It analyzes the complementarity of encryption methods, multifactor authentication, and network monitoring systems, illustrated by statistics on the success

of countering cyber threats. In conclusion, it highlights the importance of adaptability and flexibility of cybersecurity strategies for effective response to the constantly evolving cyber threats, supporting this argument with the necessity of wide adoption of comprehensive solutions at all levels of the information infrastructure of enterprises and organizations. Thus, the article offers a fundamental analysis of traffic interception threats and a review of prevalent methods for their prevention, underscoring the strategic importance of a comprehensive approach to ensuring cybersecurity in the continuously evolving digital space.

Keywords: cybersecurity, traffic interception, data encryption, multi-factor authentication, intrusion detection and prevention systems.

Введение

Одной из центральных проблем в области кибербезопасности является перехват трафика (ПТ). Многообразие методов ПТ и сложность их обнаружения требуют от организаций особого внимания к обеспечению информационной безопасности (ИБ), а об объеме ПТ и способах его предотвращения крупными международными компаниями регулярно проводятся исследования. Например, согласно материалам Kaspersky (2023 г.), выявлено, что более 30% зарегистрированных инцидентов ИБ были связаны непосредственно с ПТ [1]. Приведенные данные указывают на необходимость анализа механизмов и классификации способов ПТ, так как понимание и систематизация подобных механизмов позволяет разработать стратегии для эффективного обнаружения и предотвращения кибератак.

Соответственно, целью данной работы является анализ существующих угроз ПТ, методов их обнаружения и разработки комплексных мер защиты. Статья рассматривает различные стратегии обеспечения безопасности данных и анализирует их эффективность.

Основная часть

Международная консалтинговая компания IT Governance опубликовала отчет [2], согласно которому с ноября 2023 года по январь 2024 года количество публично раскрытых инцидентов по ПТ увеличилось на 830% (рис. 1). По данным компании IBM [3], средняя глобальная стоимость утечки данных в 2023 году составила около 4,5 миллионов долларов, что на 15% больше, чем за предыдущие 3 года.

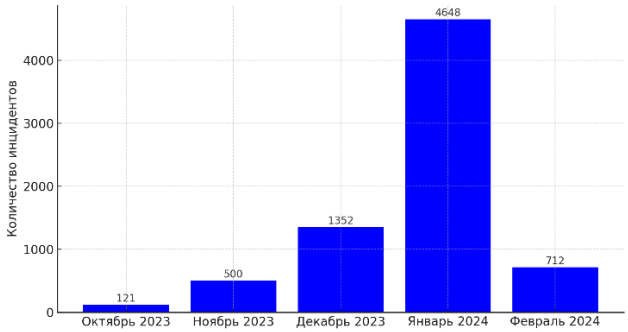

Рис. 1. Динамика роста инцидентов с ПТ [2]

Выделяют два основных вида ПТ: пассивный и активный. Пассивный перехват трафика (сниффинг), включает в себя скрытое наблюдение за трафиком без его изменения [4]. Для реализации сниффинга хакер должен иметь доступ к сети, в которой находится цель. Для этого атакующая сторона использует программное обеспечение (ПО) для мониторинга и анализа данных для незаметного сбора информации, который не оказывает влияние на работу сети или передачу данных. Примером таких ПО могут быть Wireshark или tcpdump. С их помощью злоумышленник переводит сетевую карту в режим промискуитного (смешанного) приёма. Такой прием позволяет хакеру принимать все пакеты данных, передаваемые в сети, а не только адресованные конкретному устройству.

Активный перехват трафика (АПТ) является процессом, когда киберпреступник осуществляет вмешательство в сетевой трафик с целью перехвата, модификации или перенаправления данных [5]. АПТ осуществляется

с помощью методов типа Man-in-the-Middle (MitM) атаки, Address Resolution Protocol (ARP) spoofing и Secure Sockets Layer (SSL) stripping.

MitM-атаки позволяют злоумышленнику тайно ретранслировать и изменять связь между двумя сторонами, чтобы перехватывать и изменять передаваемые данные. Для выполнения атаки хакер должен сначала обеспечить своё присутствие в коммуникационном канале между жертвой и сервером. Это может быть достигнуто через использование различных техник, например ARP spoofing в локальных сетях, Domain Name Syste (DNS) хакинг, где злоумышленник перехватывает и изменяет DNS-запросы.

ARP spoofing используется для ассоциации IP-адреса жертвы с MAC-адресом хакера, позволяя последнему перехватывать данные. SSL stripping направлен на снижение защищенности соединения, что облегчает перехват информации. Во время ARP spoofing-атаки, злоумышленник отправляет поддельные ARP-ответы на устройство отправителя. В этих сообщениях злоумышленник ложно утверждает, что IP-адрес жертвы ассоциирован с MAC-адресом хакера. Если атака успешна, устройство отправителя будет направлять трафик, предназначенный для устройства жертвы, на устройство злоумышленника.

SSL stripping является видом атаки, которая манипулирует сетевым трафиком между клиентом и сервером, принудительно понижая уровень безопасности соединения с HTTPS (защищённое) на HTTP (незащищённое). В свою очередь такой тип соединения делает данные более уязвимыми для ПТ.

Исследование (рис. 2) демонстрирует [6], что значительную часть инцидентов, связанных с ПТ, в течение года составляли MitM-атаки. Они занимают до 40% от общего числа происшествий в области ИБ. В декабре был зафиксирован наибольший всплеск активности сниффинг-атак: он составил около 60% от всех видов ПТ. Использования ARP spoofing и SSL stripping в течение всего года составило около 10% и 15% от общего количества инцидентов.

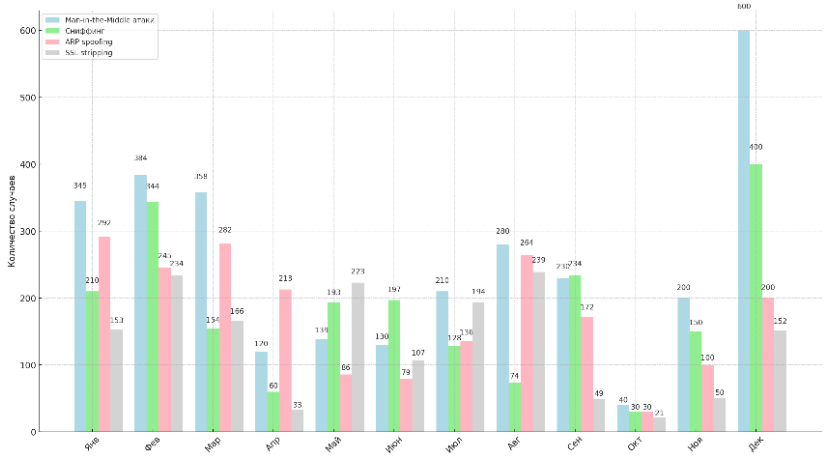

Рис. 2. Статистика инцидентов ИБ с использования методов ПТ, 2023 г. [6]

Для минимизации рисков ПТ и последующего несанкционированного доступа к данным, рассмотрим следующие методы защиты (МЗ):

- Шифрование данных с применением протоколов Secure Sockets Layer и Transport Layer Security обеспечивает создание защищённого канала между пользователем и сервером. Такое решение обеспечивает конфиденциальность и целостность передаваемой информации. Современные исследования [7] указывают на то, что использование HTTPS снижает риск MitM-атак более чем на 80%, обеспечивая надёжную защиту веб-трафика.
- End-to-end encryption (E2EE) является МЗ данных, который шифрует информацию на стороне отправителя. Данные остаются зашифрованными на всем протяжении их передачи, пока не достигнут предполагаемого получателя, у которого есть уникальный ключ для их расшифровки. E2EE шифрование активно применяется в защите сообщений в мессенджерах (например WhatsApp и Signal), электронных письмах и системах обмена файлами.
- Многофакторная аутентификация (Multi-Factor Authentication, MFA) представляет собой МЗ, который требует от пользователя предъявления двух или более доказательств своей идентичности, что существенно усложняет задачу для злоумышленника. По данным [8], внедрение MFA может снизить число успешных фишинговых атак до 99%.

- Intrusion Detection Systems (IDS) и Intrusion Prevention Systems (IPS) осуществляют мониторинг сетевого трафика на предмет аномалий. Такой инструмент защиты предоставляет возможность своевременно реагировать на потенциальные угрозы ПТ. IDS анализируют копии трафика, выявляя подозрительные действия, тогда как IPS активно блокируют обнаруженные атаки, предотвращая их распространение. Эффективность IPS достигает 95% в блокировке атак на уровне сети [9].
- Обеспечение безопасной конфигурации сетевого оборудования, включая маршрутизаторы и коммутаторы, является обязательным МЗ для противодействия ПТ. Правильная настройка и обновление ПО могут снизить риск взлома до 60%, исключая большинство векторов атак, связанных с использованием уязвимостей в устаревшем ПО [10].

Таблица 1 представляет сравнительный анализ рассмотренных МЗ от угроз ПТ. Каждый метод рассматривается с точки зрения его основных характеристик, это и аналогичные сравнения полезны для дальнейшей разработки эффективной стратегии по обеспечению безопасности компаний.

Таблица 1. Сравнительный анализ МЗ от угроз ПТ [7, 8]

Тип угрозы	**Метод защиты**	**Описание метода**	**Достоинства**	**Недостатки**
Man-in-the-Middle (MitM)	SSL/TLS и HTTPS	Шифрование канала передачи данных.	Обеспечение надежного шифрования; Поддержка на глобальном уровне.	Неустойчивость к некоторым формам атак (подмена сертификата phishing и фарминг).
ARP spoofing	Конфигурация сетевого оборудования	Защита на уровне сетевого оборудования.	Высокая эффективность предотвращения подделки ARP-адресов.	Требуется сложная настройка; Необходимо управление инфраструктурой.
Сниффинг	E2EE	Создание зашифрованного канала для пользователя.	Обеспечение анонимности; Защита от перехвата данных.	Снижается скорость соединения из-за шифрования.

SSL stripping	HSTS	Принудительное использование зашифрованных соединений.	Предотвращение снижение уровня безопасности соединения.	Требуется поддержка со стороны браузера и сервера.

Анализ представленных в таблице 1 МЗ от угроз ПТ подчеркивает их эффективность, стратегическую значимость и необходимость их интеграции в общую систему кибербезопасности. Изучение различных МЗ от угроз ПТ позволяет провести комплексный анализ их стоимости и эффективности в зависимости от размера организации. Шифрование данных с помощью SSL/TLS и использование HTTPS может быть реализовано с минимальными затратами, особенно с учетом бесплатных решений, таких как Let's Encrypt. Данные решения являются финансово доступными, а вероятность защиты от ПТ при использовании этих протоколов может достигать до 80-90% [10]. Такие факторы делают эти МЗ предпочтительным выбором для средних и малых предприятий. Конфигурация сетевого оборудования для предотвращения ARP spoofing может потребовать от компании более значительного финансирования. Внедрение данного метода может снизить риск подделки ARP-адресов на 70-80% [6]. Применение HSTS требует дополнительных затрат на поддержку со стороны сервера и может вызвать сложности в управлении для некоторых организаций. Однако, данный метод снижает вероятность успешного перехвата данных до 10-20% [11].

Анализ данных безопасности предприятий выявил, что эффективная защита информационных систем достигается за счёт комплексного использования МБ, среди которых шифрование, многофакторная аутентификация, и мониторинг сетевого трафика выступают ключевыми элементами. Такой подход не только существенно обеспечивает повышение уровня безопасности, но и приводит к заметному снижению количества успешных кибератак на корпоративные системы.

Совместное использование рассмотренных МЗ значительно повышает уровень безопасности информационных систем по сравнению с их отдельным использованием. Усиление одного метода должно сопровождаться усилением других, создавая тем самым комплексный барьер против возможных угроз перехвата данных. Такой подход подчеркивает возможность обеспечения комплексной защиты ИБ, а четкое понимание специфики каждой угрозы позволяет эффективно адаптировать эти инструменты под актуальные угрозы.

Выводы

Постоянный рост числа инцидентов, связанных с ПТ, подчеркивает необходимость постоянного совершенствования и адаптации защитных механизмов. Статистика показывает, что применение комплексного подхода, включающего шифрование, многофакторную аутентификацию и мониторинг сетевого трафика, значительно снижает уязвимости системы. Это подчёркивает необходимость широкого внедрения комплексных решений в области кибербезопасности на всех уровнях информационной инфраструктуры.

Ведение детализированной статистики по инцидентам внутри каждой компании и анализ тенденций в сфере кибербезопасности позволит управленческому составу своевременно и превентивно реагировать на изменения в методиках злоумышленников. Стратегии защиты должны быть гибкими и многоуровневыми, чтобы повысить эффективность защиты от киберугроз.

Библиографический список:

1. H2 2023 – a brief overview of main incidents in industrial cybersecurity // Kaspersky ICS CERT [Электронный ресурс]. — Режим доступа — URL: https://ics-cert.kaspersky.ru/publications/reports/2024/04/11/h2-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/ (Дата обращения: 09.04.2024).

2. Corporate Governance and Shareholding Structure Report 2023 // Eni [Электронный ресурс]. — Режим доступа — URL:

https://www.eni.com/content/dam/enicom/documents/eng/governance/shareholders-meetings/2024/Corporate-Governance-Report-2023.pdf (дата обращения: 09.04.2024).

3. Cost of a Data Breach Report 2023 // IBM [Электронный ресурс]. — Режим доступа — URL: https://www.ibm.com/reports/data-breach (дата обращения: 09.04.2024).

4. Яковишин А. Д. Применение криптографических технологий для защиты информации в облачных сервисах // International Journal of Humanities and Natural Sciences. – 2024. – том 1-2(88).

5. Яковишин А. Д. Борьба с перехватом трафика RFID и дистанционного управления: методы защиты и повышение безопасности // Современные научные исследования и инновации. – 2024. – № 1.

6. Галимов Р. Ф., Безруков П. В., Карпов М., Тюменцев Д. В., Киселев И. А. Будущее IT: как ИИ изменяет правила игры в индустрии // Информационные ресурсы России. – 2024. – №1(196). – С. 44-53.

7. Артемов А. А. МОНИТОРИНГ КАЧЕСТВА ДАННЫХ С ПОМОЩЬЮ AMAZON DEEQU // Вестник науки. – 2024. – №1(70).

8. Герасимов, А. С. Виды сетевых атак и методы защиты от них // Актуальные вопросы инноваций и современные научные открытия: Сборник научных статей по материалам II Международной научно-практической конференции, Уфа, 25 апреля 2023 года. Том Часть 2. Уфа: Общество с ограниченной ответственностью "Научно-издательский центр "Вестник науки". – 2023. – С. 171-176.

9. Зиборев А. В. АНТИПАТТЕРНЫ ПОСТРОЕНИЯ МИКРОСЕРВИСНЫХ ПРИЛОЖЕНИЙ В ВЫСОКОНАГРУЖЕННЫХ ПРОЕКТАХ // Universum: технические науки. – 2023. – №11-1(116).

10. Шайхулов Э. А., Смирнов А. П., Болдина О. Б., Азаренко Г. Ю., Благова И. Ю. Современные методы обучения информационной безопасности // Современная наука и инновации. – 2023. – №4(44). – С. 145-151.

11. Кузнецов И. А., Рубин И. М. Развитие мобильных систем рекомендаций: интеграция машинного обучения и адаптивных алгоритмов // Дневник науки. – 2024. – №3.

Оригинальность 81%