ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 343.985

MITM-АТАКА КАК СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Адамович Вячеслав Владимирович, Романова Оксана Леонидовна

Санкт-Петербургский университет МВД России, г. Санкт-Петербург
e-mail: triger228@yandex.ru, romanovvas90@mail.ru

MITM-ATTACK AS A WAY OF COMMITTING CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

Adamovich Vyacheslav V., Romanova Oksana L.

St. Petersburg University of the Ministry of Internal Affairs of Russia, St. Petersburg

Аннотация: В условиях цифровизации общества усложняется преступная деятельность. Преступники стремятся использовать информационные технологии для совершенствования механизма совершения преступления, сокрытия следов преступной деятельности, затруднения деятельности правоохранительных органов по выявлению, раскрытию и расследованию преступлений. Широкое использование информационных технологий для совершения преступных действий во многом обуславливается наличием большого количества объектов информационного воздействия со стороны преступников, что приводит к появлению вариативности способов совершения преступлений. В данной статье рассматривается «MITM-атака» как один из способов совершения киберпреступлений. Особенность указанного способа заключается в перехвате преступником информации между двумя конечными пользователями и использовании полученной таким образом информации в преступных целях. Данный тип атаки имеет множество различных вариантов ее осуществления в зависимости от выбранных средств воздействия на пользователей или эксплуатации определённой уязвимости. Эффективность данного типа атаки определяется тем фактором, при котором у двух

Abstract: In the context of digitalization of society, criminal activity becomes more complicated. Criminals seek to use information technology to improve the mechanism of committing a crime, concealing traces of criminal activity, and complicating the activities of law enforcement agencies in identifying, solving and investigating crimes. The widespread use of information technologies to commit criminal acts is largely due to the presence of a large number of objects of information influence on the part of criminals, which leads to the emergence of variability in the methods of committing crimes. This article discusses the «MITM attack» as one of the ways to commit cybercrimes. The peculiarity of this method is that the criminal intercepts information between two end users and uses the information thus obtained for criminal purposes. This type of attack has many different options for its implementation, depending on the chosen means of influencing users or exploiting a specific vulnerability. The effectiveness of this type of attack is determined by the factor in which two interacting users form the illusion of direct communication between each other, when in fact the criminal interferes with the communication process and transforms it to obtain confidential information. Various possibilities for cybercriminals to carry out an attack using this method have been studied. In particular, such methods of committing a

взаимодействующих пользователей формируется иллюзия непосредственного общения между друг другом, когда фактически преступник вмешивается в процесс коммуникации и преобразует его для получения конфиденциальной информации. Исследованы различные возможности киберпреступников по проведению атаки указанным способом. В частности, рассмотрены такие способы совершения «MITM-атаки» как взлом электронной почты, перехват сеанса, сниффинг, SSL-стриппинг, перехват Wi-Fi.

Ключевые слова: MITM-атака, киберпреступления, cookie-файлы, сниффинг, неправомерный доступ.

“MITM attack” as e-mail hacking, session interception, sniffing, SSL stripping, and Wi-Fi interception are considered.

Keywords: MITM attack, cybercrime, cookies, sniffing, unauthorized access.

Для цитирования: Адамович В.В., Романова О.Л. MITM-атака как способ совершения преступлений в сфере информационных технологий // Проблемы правовой и технической защиты информации. 2023. №11. С. 71-76.

For citation: Adamovich V.V., Romanova O.L. MITM-attack as a way of committing crimes in the field of information technology // Legal and Technical Problems Information Protection. 2023. No. 11. P. 71-76.

В настоящее время происходит активный процесс цифровизации общества, который предполагает включение информационных технологий во все сферы общественной жизни. Преступность как негативное социальное явление также активно проходит процесс цифровизации, что приводит к усложнению механизма совершения преступления в результате использования информационных технологий при его совершении. Активный рост преступлений, совершенных с использованием информационных технологий подтверждают статистические данные МВД России, согласно которым в 2020 году было зарегистрировано 510 396 преступлений, совершенных с использованием информационных технологий, в 2021 году – 517 772 преступления, в 2022 году – 522 065 преступлений, из них раскрыто в 2022 году только 142 384 преступления, остальные 73 % совершенных преступлений остались нераскрытыми [1]. Такой технологичный характер преступности затрудняет деятельность правоохранительных органов при выявлении, раскрытии и расследовании преступлений. Использование информационных технологий активно применяется преступниками в качестве способа совершения преступления, являющегося неотъемлемым элементом криминалистической характеристики. Под способом совершения преступления в теории криминалистики понимаются действия лица по подготовке к совершению преступлений, непосредственному его совершению и сокрытию следов преступления. Для преступлений, которые совершаются с использованием информационных технологий, характерно наличие всех трех элементов способа совершения преступления.

Одним из современных способов совершения преступлений, сочетающих в себе как использование аппаратно-программных средств, так и методов социальной инженерии для получения несанкционированного доступа к конфиденциальной информации пользователя является «MITM-атака». Русскоязычная расшифровка указанной аббревиатуры предполагает фразу атака «человек в середине», которая, по сути,

отражает сущность механизма совершения указанной атаки. Анохин Ю.В., Янгаева М.О. дают определение понятию «MITM-атака» как деятельности преступника, заключающейся в модификации передаваемых между сторонами данных либо совершении им противоправных действий от имени одной из сторон [2, с. 7 – 8]. «MITM-атака» предполагает проникновение киберпреступника в информационную сеть, связывающую двух пользователей, при котором он получает контроль над передаваемыми между ними данными.

Основной целью киберпреступника при совершении атаки «человек в середине» является получение неправомерного доступа к конфиденциальной информации пользователя, хищение его денежных средств, дестабилизация деятельности организации и т.д.

Данный тип атаки обладает большим количеством способов воздействия на ЭВМ, что позволяет киберпреступнику эксплуатировать различные типы уязвимостей для получения неправомерного доступа к конфиденциальной информации.

Одним из самых распространённых способов совершения «MITM-атаки» является взлом электронного почтового ящика, сущность которого заключается в осуществлении киберпреступником действий, в результате которых он получает несанкционированный доступ к электронной почте одного из пользователей, между которыми осуществляется обмен сообщениями, после чего использует получаемые сведения в целях совершения преступления [3, с. 12 – 13].

Одним из примеров, иллюстрирующих эффективное проведение MITM-атаки указанным способом, является ситуация при которой киберпреступник совершил в 2019 году хищение денежных средств в размере 1 млн. долларов посредством направления созданных или модифицированных им электронных писем в обе стороны от имени владельца израильского стартапа, а также от имени китайского фонда, в результате чего на платежные реквизиты, принадлежащие киберпреступнику был совершен крупный денежный перевод. Денежные средства были перечислены владельцем китайского фонда в качестве оплаты за первый этап разработки израильского проекта. Обнаружить факт хищения денежных средств удалось, когда владельцы израильского стартапа не получили перевод на принадлежащие им банковские реквизиты. В результате проверки пересланных друг другу электронных писем были обнаружены изменения содержания некоторых из них, а также наличие писем, которые не были созданы ни одной из сторон коммуникации. Для осуществления «MITM-атаки» киберпреступником было предварительно создано два домена, внешне сходных с оригинальными доменами израильского стартапа и китайского фонда, после чего киберпреступник, используя указанные домены, направил каждой стороне электронные письма с заголовками, находящимися в исходной переписке. Затем через созданные им поддельные домены были направлены все последующие электронные письма, при получении которых преступник обрабатывал информацию и направлял иное по содержанию электронное письмо другой стороне, что позволило ему успешно провести атаку и завладеть денежными средствами [2, с. 9 – 10].

Следующим распространённым способом совершения «MITM-атаки» является перехват Wi-Fi, сущность которого заключается в создании киберпреступником новой точки доступа Wi-Fi, маскирующейся под легитимное Wi-Fi соединение, что позволяет преступнику считывать весь интернет-трафик, проходящий через созданную им точку доступа, а также осуществлять сбор, модификацию, копирование, блокирование или уничтожение любых данных, передаваемых пользователем.

Для совершения атаки указанным способом киберпреступник определяет вектор атаки посредством поиска наиболее распространенной легитимной точки доступа, после чего им осуществляется анализ технических характеристик указанной точки, а именно: точки доступа

SSID, номера канала, MAC-адреса. После получения необходимых данных он создает точку доступа с такими же характеристиками, вынуждая пользователя подключиться к фиктивной точке доступа Wi-Fi, что позволяет киберпреступнику осуществлять слежение за сеансом пользователя, а также считывать и модифицировать передаваемые пользователем пакеты данных в целях получения неправомерного доступа к конфиденциальной информации [4, с. 26-27].

Перехват сеанса также является одним из способов совершения «MITM-атаки» и предполагает слежение со стороны киберпреступника за действиями пользователя, направленными на авторизацию пользователя на каком-либо сайте, после чего киберпреступником осуществляются действий направленные на перехват cookie-файлов сеанса для входа в ту же учётную запись, принадлежащую пользователю, через используемый киберпреступником браузер. Значимость для киберпреступника перехвата cookie-файлов заключается в их сущности, предполагающей отправку на web-сервер хранящегося на компьютерном устройстве пользователя фрагмента данных, позволяющих идентифицировать его на web-сайте и предоставить доступ к принадлежащей ему учетной записи [5, с. 49-50]. Идентификатор сеанса представляет собой неотъемлемый элемент функционирования cookie-файлов, предполагающий некоторую случайную строку, состоящую из буквенных и цифровых символов, которая позволяет идентифицировать пользователя с конкретным фрагментом данных, в связи с чем завладение идентификатором сеанса со стороны киберпреступника приводит к возникновению у него возможности совершить вход в учетную запись пользователя вместо него. После завладения идентификатором сеанса киберпреступник способен получить доступ к любой информации о пользователе на указанном веб-сайте, осуществлять действия от имени пользователя, в том числе направленные на хищение денежных средств.

Одним из способов совершения «MITM-атаки» посредством перехвата сеанса является фиксация сеанса, при которой киберпреступник осуществляет эксплуатацию уязвимости, дающей возможность установить конкретный идентификатор сеанса, принадлежащий другому пользователю, что создает условия для получения всех конфиденциальных данных пользователя при его переходе на какой-либо интернет-ресурс с использованием идентификатора сеанса, принадлежащего самому киберпреступнику [2, с. 10 – 11]. Данный способ атаки позволяет киберпреступнику максимально упростить действия по завладению идентификатором сеанса. Реализация указанного типа атаки возможна посредством использования одного из методов социальной инженерии в виде фишинга, при котором на электронную почту пользователя отправляется сообщение, содержащее ссылку с определенным идентификатором сеанса, принадлежащего киберпреступнику, что позволяет ему установить контроль над используемым пользователем идентификатором сеанса в случае перехода пользователя по ссылке.

Иным способом совершения «MITM-атаки» посредством перехвата сеанса является использование программ-снифферов, которые позволяют анализировать сетевой трафик пользователя, включая передаваемые им пакеты данных, к которым относятся cookie-файлы, что создает киберпреступнику благоприятные условия для получения доступа к указанным файлам и их дальнейшего использования в целях совершения иных преступлений [6, с. 635-636].

Возможность совершения «MITM-атаки» посредством перехвата сеанса возникает и при использовании киберпреступником подмены протокола разрешения адресов, получившее название ARP-spoofing, что позволяет киберпреступнику осуществлять действия

по отправлению ложных ответов ARP по заданному IP-адресу, в результате чего происходит наполнение ARP кэша технического устройства пользователя MAC-адресом технического устройства злоумышленника вместо MAC-адреса локального маршрутизатора [7, с. 98-99]. Данное обстоятельство приводит к возникновению ситуации, при которой, по сути, техническое устройство киберпреступника выступает в роли прокси-сервера, что дает возможность киберпреступнику непосредственно перед отправкой данных просматривать их или изменять в целях совершения преступлений, таких как переадресация пользователя на фишинговый сайт.

Еще одним способом осуществления «MITM-атаки» является SSL-стриппинг, предполагающий совершение киберпреступником действий по перехвату сигнала TLS и последующей его модификации в целях снятия уровня защиты с протокола шифрования HTTPS и его замены незащищенным протоколом HTTP, что позволяет киберпреступнику получить неправомерный доступ к сеансу пользователя. [5, с. 50-51]

Так, постоянное совершенствование способов совершения киберпреступлений в том числе и нахождение киберпреступниками новых векторов атаки типа «человек в середине» создаёт условия, затрудняющие деятельность органов предварительного расследования по их выявлению, пресечению и расследованию. Однако несмотря на высокий уровень конспирации преступной деятельности со стороны киберпреступников остаются определённые следы их цифрового присутствия, которые требуют соответствующего процессуального закрепления в качестве доказательств по уголовному делу, в связи с чем требуется формирование специальных знаний у сотрудников правоохранительных органов по выявлению и расследованию киберпреступлений, совершенных указанным способом. В целях усвоения сотрудниками правоохранительных органов соответствующих знаний и формирования у них умений по расследованию преступлений указанной группы необходимо проведение информационно-разъяснительной работы в виде специальных курсов, лекций и семинаров, целью которых является профилирующее изучение киберпреступлений.

Библиографический список

1. *Статистические данные ГИАЦ МВД России. [Электронный ресурс]. – URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 22.09.2023).*
2. *Анохин Ю.В., Янгаева М.О. К вопросу о MITM-атаке как способе совершения преступлений в сфере компьютерной информации // Философия права. 2021. № 2(97). С. 7-13.*
3. *Антонян Е.А., Клещина Е.Н. Киберпреступность на современном этапе: тенденции и направления противодействия // Вестник экономической безопасности. 2022. № 5. С. 11-15.*
4. *Аитов А.И. Организация MITM-атаки через общественную беспроводную точку доступа // Студенческий вестник. 2021. № 21-8(166). С. 26-28.*
5. *Мотылец А.А., Фешина Е.В., Василенко И.И., Куштанок С.А. Реализация инструментов для MITM-атаки и ее проведение в виртуальной среде // Наука XXI века: проблемы, перспективы и актуальные вопросы развития общества, образования и науки: международная межвузовская осенняя научно-практическая конференция : сборник материалов и докладов, Яблоновский, 27 октября 2021 года. Яблоновский: ФГБУ «Российское энергетическое агентство» Минэнерго России Краснодарский ЦНТИ- филиал ФГБУ «РЭА» Минэнерго России, 2021. С. 48-53.*
6. *Кодацкий Н.М., Мотуз А.С. Угрозы кибербезопасности в информационной среде // Studnet. 2022. № 1. С. 633-639.*
7. *Брюхнов А.А., Марков А.И., Петренко А.В. Характеристика преступности в сфере высоких технологий и ее предупреждение // Философия права. 2021. № 3(98). С. 96-101.*
8. *Колчевский И.Б., Бицадзе Г.Э. Преступления в сфере информационных*

технологий: понятие, структура // Научный портал МВД России. 2021. № 2(54). С. 40-47.

9. Алиев Т.Ф. Вопросы противодействия преступлениям, совершаемым с использованием IT-технологий // Юридические исследования. 2023. № 10. С. 100-107.

10. Батюкова В.Е. К вопросу о характеристике киберпреступлений в банковской сфере // Вестник экономической безопасности. 2021. № 1. С. 100-102.