УДК 004.056.53

Анализ атак в информационных системах

Ю.П. Преображенский✉, И.А. Еременко, С.В. Зяблов

Воронежский институт высоких технологий, Воронеж, Россия

В данной работе проведено рассмотрение основных видов сетевых атак в информационных системах. Осуществлено детальное рассмотрение каждой из атак. Материалы статьи могут быть использованы для обеспечения максимальной защиты персонального компьютера, подключенного к сети, и личных данных пользователя этого компьютера. Трудность при выявлении удалённой атаки и относительная простота осуществления вследствие избыточной функциональности современных систем выводит подобный вид неправомерных действий на первое место по степени опасности и препятствует своевременному реагированию на осуществлённую угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

Ключевые слова: информационная безопасность, защита информации, информационная система, компьютерная сеть, компьютерная атака.

Analysis of attacks in information systems

Yu.P. Preobrazhenskiy✉, I.A. Eremenko, S.V. Zyablov

Voronezh Institute of High Technologies, Voronezh, Russia

In this paper, the main types of network attacks in information systems are considered. A detailed review of each of the attacks has been carried out. The article can be used to ensure maximum protection of a personal computer connected to the network and personal data of the user of this computer. The difficulty in identifying how a remote attack is carried out and the relative ease of implementation due to the excessive functionality of modern systems puts this type of illegal actions in the first place in terms of danger and prevents timely response to the threat, as a result of which the violator increases the chances of successful implementation of the attack.

Keywords: information security, information protection, information system, computer network, computer attack.

Под кибератакой понимается предумышленно организованная совокупность действий с участием программно-технических средств, направленная на нанесение экономического, технического или информационного ущерба.

Модель облачных услуг разделена на три типа: инфраструктура как услуга (IaaS), программное обеспечение как услуга (SaaS) и платформа как услуга (PaaS).

Модель развертывания основана на типе доступа к облаку: публичная, частная и гибридная. Облачные вычисления имеют много потенциальных угроз, которые классифицируются как:

– злоупотребление использованием облачных вычислительных ресурсов;

– атаки на данные: вредный инсайдер, киберворовство в интернете;

– атаки на безопасность облаков: атаки с инъекцией вредоносного программного обеспечения, атаки в обертке.

Поскольку доступ к критическим услугам осуществляется с сервера по сети, необходимо обеспечить доступность этих услуг для легитимного пользователя, при этом злоумышленники будут препятствовать доступу. Примером таких преград является злоупотребление использованием облачных вычислительных ресурсов

атакующими. Злоумышленники прерывают или отказывают в предоставлении услуг легитимному пользователю с помощью атаки «Отказ в обслуживании» (DoS).

Атака «Отказ в обслуживании» – это тип кибератаки, во время которой злоумышленник пытается сделать сервер или другое устройство недоступным для пользователей, прерывая его нормальное функционирование.

Атаки DoS, как правило, действуют путем перегрузки или заполнения целевой машины запросами, пока сервер не потеряет возможность обрабатывать все запросы, что приводит к отказу в обслуживании. DoS-атака характеризуется использованием одного компьютера для запуска атаки. Атака, которая поступает из многих источников, называется «распределенная атака на отказ в обслуживании» (DDoS). Во время проведения DoS атаки злоумышленник пытается достичь одну или обе из следующих целей [1, 2]:

– Нарушить подключение законного пользователя из-за истощения пропускной способности, мощностей обработки маршрутизатора или сетевых ресурсов.

– Нарушить предоставление услуг законному пользователю, истощив ресурсы сервера (например: сокеты, ЦП, память, пропускная способность диска/базы данных и пропускная способность ввода/вывода). Они включают атаки флудинга на прикладном уровне (application-level flooding attacks). Для достижения цели злоумышленник обычно пользуется одним из двух типов атак: атака переполнения буфера или атаки флуда. Тип атаки, при котором происходит переполнение буфера памяти, изображенное на рисунке 1, может привести к тому, что машина начинает потреблять все доступное пространство на жестком диске, памяти или времени ЦБ. Эта форма эксплойта часто приводит к вялому поведению, системным сбоям или другим вредным действиям сервера, что приводит к отказу в обслуживании.

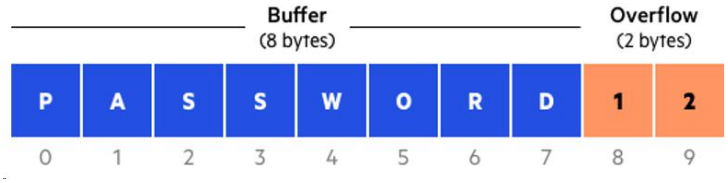

Рисунок 1. Переполнение буфера

Отправляя на целевой сервер множество пакетов, злоумышленник может перенасыщать мощность сервера, что приводит к отказу в обслуживании. Схематически атака флуда изображена на рисунке 2.

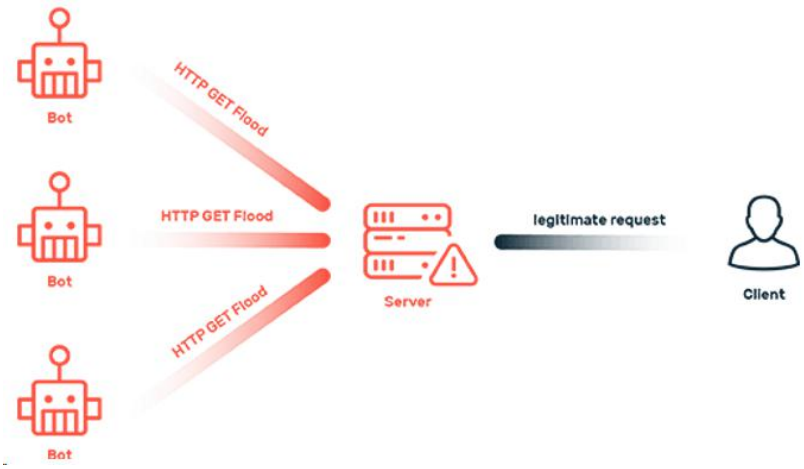

Рисунок 2. HTTP Flood Attack

Отличительной разницей между DDoS и DoS является количество соединений, использованных во время атаки. Некоторые атаки DoS, такие как медленные атаки на отказ в обслуживании, такие как Slowloris, имеют свою силу в простоте и минимальных требованиях, необходимых для их эффективности.

DoS использует одно соединение, тогда как DDoS атака использует множество источников трафика атаки.

Среди киберпреступников и организованных преступных групп распределенные атаки отказа в обслуживании приобретают все большую популярность. Эти организации объединились в сложные иерархии и структуры для координации и усугубления последствий атаки. Кроме того, эти группы иногда используют свою организацию для совершения преступлений с вымогательством или другими схемами нелегального заработка.

DDoS-атаку характеризует огромное количество скомпрометированных источников из одновременно запускаемой атаки на веб-сервер, чтобы отказать действительным пользователям в предоставлении услуг. DDoS-атака является очень простым, но мощным типом атаки, которая перегружает пропускную способность сети и количество возможных подключений на постоянной или временной основе. Поток трафика во время атаки DDoS внешне легитимен, поэтому становится трудно отличить запросы законного пользователя от запросов злоумышленника. В последнее время DDOS-атаки стали очень серьезной опасностью для облачных, мобильных и веб-приложений [3]. Как правило, DDoS-атака запускается злоумышленником из набора скомпрометированных систем, известных как ботнет. Схематически ботнет изображен на рисунке 3.

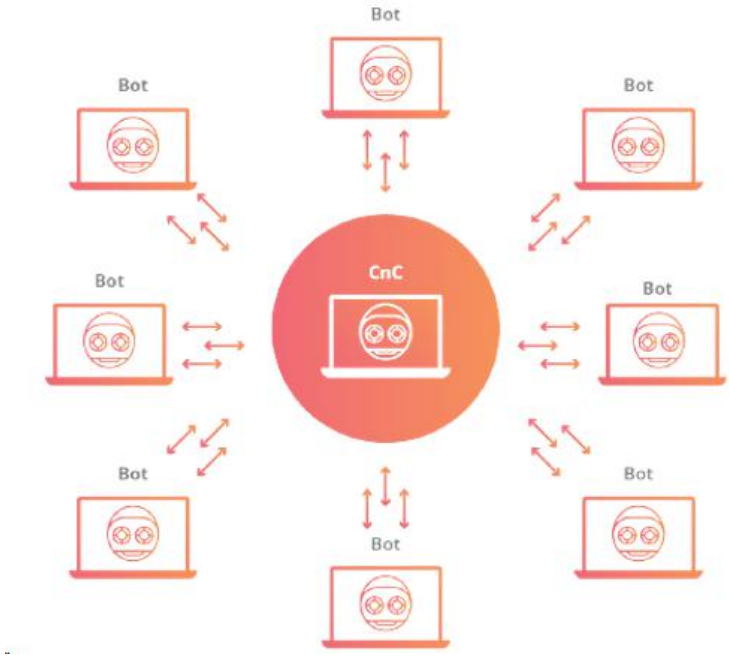

Рисунок 3. Ботнет

Для атаки злоумышленник использует технологию клиент-сервера. В целом DDoS-атака состоит из мастер-программы, обработчика, агентов и жертвы. Зомби (агенты или боты) – это машины, которые использует мастер-программа для формирования ботнета. Чем больше зомби, тем разрушительнее будет атака. Кроме того, связь между злоумышленником и агентами осуществляется посредством обработчиков. С помощью них злоумышленник посылает команды для управления

ботнетом. Фактически атаку совершают скомпрометированные компьютеры, объединенные в ботнет.

Злоумышленник использует много методов сканирования для поиска уязвимых к атакам машин. Наиболее уязвимым уровнем стека OSI и TCP/IP для DDoS-атаки являются транспортный уровень (уровень 3 OSI) и сетевой уровень (уровень 4 стека OSI и TCP/IP) системы связи. Атаки, направленные на эти уровни, предназначены для заполнения сетевого интерфейса трафиком атаки, чтобы перегрузить его ресурсы и лишить способности реагировать на законный трафик [4]. Кроме того, атаки прикладного или седьмого уровня теперь становятся более популярными и сложными для противодействия видами атак DDoS, потому что трафик во время них почти подобен законному. Но их исполнение усложняется и для злоумышленника – для начала необходимо установить подлинное соединение с жертвой.

Атаки прикладного уровня направлены на уровень 7 стека OSI, который обращается непосредственно к конечному пользователю, предоставляя доступ к сервисам, к которым обращается пользователь. Более того, этот слой считается наиболее достижимым и наиболее заметным для внешнего мира в сети. DDoS-атака прикладного уровня создает меньше сетевого трафика, чем атаки других уровней, так что обнаружить ее становится труднее [5]. Кроме того, она приводит больше накладных расходов на систему с эквивалентным объемом трафика вредоносных запросов на стороне сервера и показывает большую возможность обойти системы вторжения и обнаружения, чем традиционная DDoS-атака.

С увеличением вычислительной сложности в интернет-приложениях и большей пропускной способностью сети ресурсы сервера могут стать узким местом для этих программ. Этот тип атаки может использовать меньше компьютеров-ботов, но атака наносит большой ущерб веб-сайту.

Перед началом обмена информацией с помощью TCP, между двумя компьютерами необходимо установить стабильную связь. Это происходит с помощью «трехэтапного рукопожатия». Первый компьютер отправляет второй пакет с SYN битом, что означает предложение создать соединение. Второй компьютер отправляет обратный пакет с битами ACK и SYN в знак подтверждения. Первый компьютер соответствует пакету с ACK битом, чем инициирует соединение. Теперь компьютеры готовы обмениваться информацией.

Пока информация отправляется с помощью TCP, принимающая сторона должна соответствовать пакету с битом ACK на каждый принятый пакет с данными. Числа номера в последовательности и ACK являются частью заголовка TCP и помогают компьютерам отслеживать, какие данные были утрачены, а какие отправлены дважды или приняты не в свою очередь [6].

Для инициации завершения соединения первый компьютер отправляет пакет с установленным битом FIN. Второй соответствует пакету с битами FIN и ACK, на что первый компьютер соответствует пакету с битом ACK и завершает соединение.

TCP связь может определять утраченные пакеты, используя таймер. После отправки пакета отправитель запускает таймер и помещает пакет в очередь повторной передачи. Если таймер закончился, а отправитель еще не получил подтверждения от получателя, он снова отправляет пакет. Процесс соединения изображен на рисунке 4.

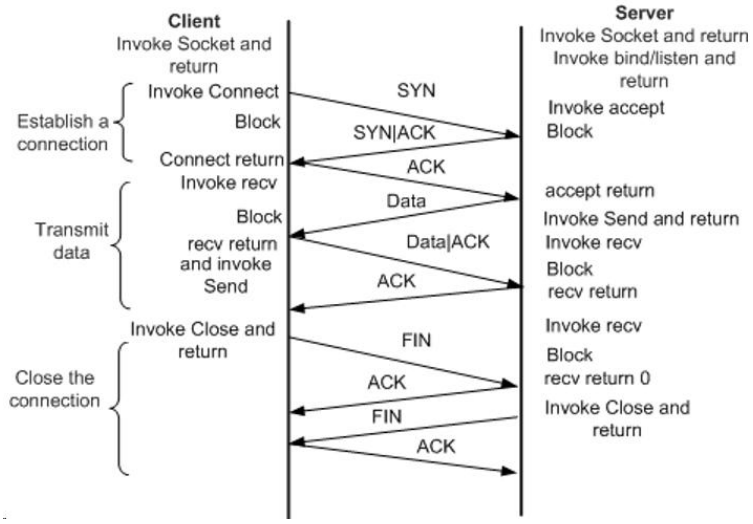

Рисунок 4. TCP соединение/разъединение

HTTP DDoS-атаки – это атаки уровня программ в системе. Эти атаки преследуют цель сделать онлайн-сервисы недоступными для законных конечных пользователей.

Атаки с переполнением HTTP – это атаки уровня приложений и сосредоточены на заполнении чрезмерным запросом на веб-сервер, чтобы перегрузить веб-сервер и сделать его не в состоянии обработать входящие запросы. Впоследствии работа сервиса будет прекращена.

DoS или ReDoS используют специально созданное сообщение с регулярным выражением для использования недостатка в библиотеке программного обеспечения на стороне сервера. Недостаток позволяет серверу тратить свои ресурсы на вычисление регулярного выражения на основе вводимой пользователем информации.

Атаки с коллизией хеширования используют общие недостатки безопасности во фреймворках веб-приложений. Хэш-таблицы создаются на серверах приложений для индексации параметров POST. При возврате сравнимых значений хеширования серверы приложений должны управлять коллизией хеширования. Операции разрешения коллизий потребляют дополнительное процессорное время, например, когда злоумышленник посылает сообщения POST с большим количеством аргументов в сценариях DoS-атаки с коллизией хеширования. Коллизии хэша DoS-атак чрезвычайно успешны [7]. Они могут производиться даже с одной машины, постепенно истощая ресурсы сервера.

Атаки HTTP флудинга являются наиболее распространенными DDoS-атаками, направленными на ресурсы сервера. Эти атаки выглядят как обычные HTTP-запросы GET или POST к веб-серверу жертвы, что затрудняет их идентификацию. Атаки HTTP флудинга часто включают в себя большое количество компьютеров-ботов. Эти боты делают многочисленные запросы на целевой сайт, чем приводят к DoS. Во время атак HTTP GET флудинга, злоумышленники могут посылать различные HTTP-запросы на веб-сервер. Веб-сервер может иметь несколько подключений от одного клиента к одному серверу. Каждому клиентскому процессу будет назначен новый номер порта. Этот процесс позволяет выполнять несколько одновременных запросов на один веб-сайт с одного компьютера. Злоумышленники могут нацеливать свои запросы на главную веб-страницу, случайную веб-страницу, другие ресурсы, например файлы изображений или на их комбинацию. В отличие от массовых атак с высокой пропускной способностью, атаки с низкой пропускной способностью, совершаемые

злоумышленниками на прикладном уровне, полагаются на атаки Slow Read во избежание обнаружения [8]. Нет необходимости в армии ботов, поскольку этот тип атаки можно осуществить только с одной машиной и использовать меньшую пропускную способность по сравнению с традиционными атаками флудинга. Во время медленных атак такого типа трафик выглядит как законный. Клиент HTTP – это веб-браузер, устанавливающий соединение с сервером для передачи одного или нескольких сообщений с запросом HTTP.

Дифференциация трафика такой атаки и обычного трафика представляет собой сложную задачу и требует опыта в этой области.

Выводы. Таким образом, было проведено рассмотрение основных сетевых атак. Указанная область может считаться как наиболее развивающейся, поскольку наблюдается непрерывное соперничество среди злоумышленников и организаций, обеспечивающих безопасность данных. Несмотря на возможное использование комплексных мер по защите компьютера, наиболее надежным способом защиты является применение проверенных электронных ресурсов, чтение писем из проверенных источников. То есть обеспечение наибольшей защиты от атак может быть достигнуто самим пользователем при соблюдении мер предосторожности.

СПИСОК ИСТОЧНИКОВ

1. Львович Я.Е. Об анализе эффективности идентификации атак на беспроводные сенсорные сети / Я.Е. Львович, Ю.П. Преображенский, Е. Ружицкий // Вестник Воронежского института высоких технологий. – 2022. – № 3 (42). – С. 107-109.

2. Аветисян Т.В. Особенности информационных систем на предприятиях / Т.В. Аветисян, Я.Е. Львович, А.П. Преображенский // Вопросы науки. – 2023. – № 2. – С. 8-15.

3. Лапина Т.И. Управление доступом к информационным ресурсам в информационных системах / Т. И. Лапина, Э.М. Димов, Е.А. Петрик, Д.В. Лапин // Моделирование, оптимизация и информационные технологии. – 2018. – Т. 6. – № 4.

4. Аветисян Т.В. О характеристиках безопасности в информационной системе / Т.В. Аветисян // Технологии и техника: пути инновационного развития: сборник научных статей Международной научно-технической конференции. – Воронеж, 2023. – С. 39-42.

5. Львович И.Я. О проблемах передачи информации в информационных системах / И.Я. Львович // Оптимизация и моделирование в автоматизированных системах: труды Международной молодежной научной школы, Воронеж, 08–10 февраля 2023 года / отв. редактор Я.Е. Львович. – Воронеж, 2023. – С. 50-53.

6. Нагорнов Н.М. О проблемах обеспечения надежности информационно-телекоммуникационных систем / Н.М. Нагорнов, Р.Т. Минигубаев, Ю.П. Преображенский // Инновационный потенциал развития общества: взгляд молодых ученых: сборник научных статей 4-й Всероссийской научной конференции перспективных разработок, Курск, 01 декабря 2023 года. – Курск, 2023. – С. 217-220.

7. Львович Я.Е. Проблемы обеспечения информационной безопасности распределенных информационных систем / Я.Е. Львович, Ю.П. Преображенский // Вестник Воронежского института высоких технологий. – 2022. – № 4 (43). – С. 68-71.

8. Мельникова Т.В. Анализ некоторых экспериментальцых подходов для беспроводных систем связи / Т.В. Мельникова, В.В. Воробьева, Е. Ружицкий // Вестник Воронежского института высоких технологий. – 2020. – № 3 (34). – С. 34-37.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Преображенский Юрий Петрович, кандидат технических наук, доцент, проректор по информационным технологиям, Воронежский институт высоких технологий, Воронеж, Россия.
e-mail: petrovich@vivt.ru

Еременко Иван Анатольевич, студент, Воронежский институт высоких технологий, Воронеж, Россия.
e-mail: 28Eremenko90@mail.ru

Зяблов Сергей Владимирович, студент, Воронежский институт высоких технологий, Воронеж, Россия.
e-mail: Zyablov7SV@mail.ru