РАЗДЕЛ V. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056

ВРЕДОНОСНЫЕ ПРОГРАММЫ В КОМПЬЮТЕРНЫХ СЕТЯХ: DDOS-АТАКИ И ИХ ПОСЛЕДСТВИЯ

© 2020 Василенко К.А.[1], Золкин А.Л.[2], Абрамов Н.В.[3], Курганов Д.О.[3]

[1]Владивостокский государственный университет экономики и сервиса, г.Владивосток, Россия
[2]Средневолжская специализированная производственная база, г. Самара, Россия
[3]Дальневосточный федеральный университет, г.Владивосток, Россия

Настоящая статья посвящена исследованию проблем, связанных с угрозой, исходящей от вредоносных программ в компьютерных сетях, таких как непосредственно DDOS-атаки; выявлены особенности таких программ, а также приведены способы, позволяющие с ними бороться. Следует констатировать, что всемирная сеть Интернет сегодня уже не рассматривается как полноценное безопасное информационное поле для пользователей. Связано это прежде всего с тем, что современные антивирусные программы в отношении скорости отстают по модернизации и не «успевают» за развитием новых вредоносных программ, атак и взломов, несмотря на постоянное обновление защитной базы. В настоящий момент непосредственно рабочая станция обычного пользователя используется злоумышленником в собственных интересах с целью атаковать более крупную информационную «кибержертву». Необходимо, чтобы защитный способ от вредоносных программных атак заблаговременно уже на стадии его разработки создавался с учетом указанных обстоятельств.

Ключевые слова: компьютерные сети, web-сервер, вредоносные программы, DDOS-атаки, информация, информационная безопасность.

На современном этапе развития рынка услуг по защите информации все большую актуальность приобретает проблема защиты WEB-сервера от так называемых DDOS-атак. В переводе с английского DDOS (Distributed Denial of Service) означает распределенный отказ в обслуживании. «Такой» способ атаки имеет своей целью вывод из штатного рабочего состояния атакуемую вычислительную машину. Как правило, данный вид атаки применяется в качестве инструмента для шантажа, ликвидации конкурентов, либо банально, как забавная деятельность у начинающих хакеров. DDOS-атака представляет собой на сегодня масштабную угрозу для всемирной сети Интернет и уже возымела статус «кибертерроризма».

Причина всему происходящему – легкодоступность осуществления данного вида атаки, поскольку чтобы достичь поставленной цели злоумышленник должен перенаправить трафик с множества зараженных компьютеров на атакуемый сервер. Реализовать это не так сложно, можно ограничиться лишь написанием скрипта с использованием языка JavaScript, загружающего сколько угодно раз WEB-страницу с атакуемого сервера, и размещением этого скрипта на посещаемой странице какого-нибудь WEB-сайта [10].

Если данный ресурс отсутствует, то злоумышленник очень просто сделает фейковый сайт и осуществит спам-рассылку, содержащую ссылку на страницу с вредоносным кодом. В итоге из-за скопления пользователей создастся множество запросов, от которых сервер оказывается просто перегружен при попытке их обработки [2, 3].

Приведенный выше пример демонстрирует способность вывода из рабочего состояния сайтов со средним уровнем вычислительной мощности. Для произведения атаки самых мощных серверов, как ,например, сайт радиостанции «Эхо Москвы» 4 мая 2012 года, злоумышленники применили так называемый «BOT-NET», представляющий собой сеть, состоящую из зараженных компьютеров. При этой атаке были использованы три зомби-сети, в совокупности состоящих из трехсот пятнадцати тысяч зараженных компьютеров.

Однако обычным повышением вычислительной мощности сервера для увеличения безопасности сервера при масштабной DDOS-атаке не обойдется, поскольку зачас-

тую ширины Интернет-канала сервера бывает недостаточно для пропуска всех поступающих на сервер запросов. В результате страдают простые пользователи, просто простаивающие в очереди в ожидании, когда высвободится канал и будет получен доступ к серверу.

Вопрос решения указанной проблемы находится в поле зрения многих ученых мира. Сотни компаний производят разнообразные программные и аппаратные способы защиты. Системные администраторы постоянно разрабатывают обновленные алгоритмы, способные фильтровать трафик, поступающий на сервер.

Ниже рассмотрим основные методы решения обозначенной проблемы, применяемые на современном этапе. Новый метод защиты сервера от масштабных атак разработали американские ученые из Вашингтонского университета К. Диксон и Т. Андерсон [2, 10]. Их авторский метод базируется на создании облака из нескольких тысяч компьютеров, настроенных на прием перенаправленных отфильтрованных запросов зараженных машин, а сервер, в свою очередь, займется обработкой запросов, поступающих только от легитимных пользователей [3]. Указанный комплекс получил название Phalanx [10].

Позиция ученых заключается в том, что разработанная технология позволяет сдерживать атаки практически любой силы, достаточно только увеличения количества компьютеров в данном облаке. Также данный комплекс может замедлить работу BOT-NET, поскольку каждый компьютер, пытающийся получить доступ к серверу, должен решить несложную задачу, а это влечет за собой существенное замедление в работе BOT-NETa.

Защиту от DDOS-атаки обеспечивают системные администраторы и специалисты в области информационной безопасности как на аппаратном, так и на программном уровнях доступа к серверу. Анализируя программный уровень защиты, приведем пример исследования проведенного Слеповичевым И.И. Исследователь предложил метод решения проблемы, реализуемый на программном уровне, с использованием математического аппарата нечеткой логики и нейронных сетей [8]. Целью работы ставилось создание программы, позволяющей обнаруживать DDOS-атаки в выявлении нелегитимных пользователей. Но главный эффект от использования данной программы заключается в том, что она может обучаться и пресекать любые новые методы воздействия на сервер со стороны злоумышленника, поскольку программа в состоянии пополнять свою базу знаний по выявлению новых алгоритмов формирования запроса злоумышленником для представления их системе как запросов от легитимных пользователей. Данный способ эффективен, но для его реализации необходимы более мощные вычислительные ресурсы, чем для стандартной методики фильтрации запросов [6]. В итоге рядовым некоммерческим сайтам, а также сайтам малого бизнеса нерентабельно использование данного способа, поскольку затраты на закупку аппаратных средств для повышения ресурса вычислительной мощности сайта в целом довольно высоки.

В основе политики безопасности больших корпораций, таких как «Google», «Yandex»,«Facebook», «Вконтакте», находится система «распределенных серверов», которая отличается от обычной развернутостью и функционированием в пространстве. Целью данной системы является организация параллельно функционирующей сети серверов (дата-центров), выполняющей совокупную обработку поступающей от клиентских компьютеров информации посредством распределения нагрузки и на вычислительные ресурсы, и на пропускную способность каналов связи. Такая методика довольно эффективна, поскольку сервера не находятся в одном здании, а располагаются в разных городах (странах), используя и занимая ресурс местных провайдеров для доступа в сеть Интернет [4]. Следовательно, в совокупном использовании ширина канала Интернета такого WEB-сайта будет гораздо более устойчивой:

$$S = \sum P_n ,$$

где P– ширина канала Интернет, предоставляемая провайдером для сервера,
а n –количество провайдеров.

Таким образом, S – это общая ширина канала Интернет-сайта, построенного по такой методике. Но нужно отметить, что данная систе-

ма слишком дорогостоящая и нерентабельная для сайтов даже среднего бизнеса.

Обобщая аналитическую информацию о приведенных современных и наиболее эффективных методах защиты от «распределенного отказа в обслуживании», можно сделать один общий вывод о том, что абсолютного решения для всех видов (классов) проектов по данному типу атаки не существует [9].

Основная причина кроется в материальной составляющей всех методик. Эффективность методики защиты напрямую зависит от величины материальных затрат владельца ресурса. Следовательно, и риск угрозы для малобюджетных сайтов крайне высок, а создание новых, более эффективных методик защиты основано лишь на повышении материальных затрат для их реализации.

Рассмотрим актуальные проблемы в DDOS-атаках. Атаки, приводящие к распределенному отказу в обслуживании, становятся все более громоздкими, а пропускная способность, предоставляемая провайдерами, меняется крайне медленно.

Политика безопасности провайдеров на современном этапе при превышении размера ширины канала ведет к полной блокировке клиента и его полному отключению от сети.

В такой ситуации провайдеры объясняют это недостаточными ресурсами вычислительной мощности для работы с большими размерами поступаемого трафика. Имеет смысл в данном случае заблокировать клиента до момента снижения поступаемых запросов (трафика) не выше 70-80% от ширины канала, предоставляемого клиенту [1].

Такая политика безопасности вполне оправдана со стороны провайдера, поскольку нет необходимости в огромном количестве вычислительной мощности на анализ запросов, поступающих из сети. Учитывая, что ширина поступающего трафика при атаке выше, чем ширина канала сервера, то, следовательно, некоторая масса запросов останется на стороне провайдера в ожидании своей очереди, занимая ресурсную емкость его вычислительной мощности и подвергая угрозе всех остальных клиентов.

Однако применительно к WEB-ресурсу (сайту) данная методика губительна, поскольку вычислительной мощности сервера с учетом программной фильтрации запросов часто хватает для обработки запросов, поступающих по каналам связи и предоставляемых его провайдером, а ширина канала в этот момент полностью загружена [5, 7].

Таким образом, роль такой защиты на уровне провайдера убивает всю суть методики защиты на уровне WEB-сервера, приводя к простаиванию сервера в офлайн-режиме для его легитимных пользователей.

Подытоживая изложенное выше, можно сделать вывод о том, что для защиты WEB-серверов от атак «распределенного отказа в обслуживании» следует не только выстраивать политику анализа, фильтрации и дополнительной вычислительной мощности, но и разрабатывать новую политику предоставления доступа сети Интернет провайдерами. Кроме этого, необходимо также создать новую методику увеличения ширины канала связи, предоставляемую WEB-серверу его провайдером.

В итоге пропускная способность канала связи сделает возможным поступление большего количества трафика на WEB-сервере, позволяя бороться с данной атакой комплексно, подключая при этом программную фильтрацию со стороны сервера и позволяя уменьшить нагрузку на каналы связи.

СПИСОК ИСТОЧНИКОВ

1. Аладышев О.С., Овсянников А.П, Шабанов Б.М. Развитие корпоративной сети Межведомственного суперкомпьютерного центра. - URL: vbakanov.ru›metods/1441/ (Дата обращения: 22.12.2019).

2. Андреев Д.А. Разработка и исследование риск-моделей SYNflood-атак на серверы компьютерных систем: диссертация ... кандидата технических наук. – Воронеж, 2008. – 118 с.

3. Золкин А.Л., Просвиров Ю.Е., Ворошилов Э.А. Разработка структурной схемы автоматизированной системы контроля технического состояния коллекторов тяговых электродвигателей //Вестник Ростовского государственного университета путей сообщения. – 2009. - № 1. – С. 45-51.

4. Золкин А.Л., Тычков А.С., Калякулин А.Н. Возможности применения и особенности использования свободно распространяемого программного обеспечения в образовательном процессе// Актуальные проблемы развития транспортного комплекса: Материалы VI Всероссийской дистанционной научно-практической конференции. – Самара: СамГУПС, 2010. – С. 63-66.
5. Золкин А.Л. Разработка информационно-управляющей системы для контроля износа коллекторов тяговых электродвигателей// //Вестник Донецкой академии автомобильного транспорта. – 2019. - № 2. – С. 65-74.
6. Панкратов С.А. Использование графической информации для защиты программного и информационного обеспечения // Инженерный вестник Дона. - 2012. - №2. - URL:ivdon.ru/ru/magazine /archive/n2y20 12/792/ (Дата обращения: 22.12.2019)
7. Патент на полезную модель № 89248, МПКG01R 31/34, H01R 39/58. Автоматизированная система учета, контроля и прогнозирования износа коллекторов тяговых электродвигателей локомотивов/ А.Л. Золкин, Ю.Е. Просвиров. - №2008147230/22; Заявлено 02.12.2008; Опубл. 27.11.2009; Приоритет 02.12.2008.
8. Слеповичев И.И., Ирматов П.В., Комарова М.С., Бежин А.А. Обнаружение DDoS-атак нечеткой нейронной сетью // Известия Саратовского университета. Серия: «Математика. Механика. Информатика». - 2017. - № 3. - С. 84–89.
9. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. - М.: Лори, 2016. - 480 с.
10. Phalanx: Withstanding Multimillion-Node Botnets - http://static.usenix.org/event/nsdi08/tech/full_papers/dixon/dixon_html (Дата обращения: 25.01.2020).

MALICIOUS SOFTWARE IN COMPUTER NETWORK: DDOS ATTACS AND THEIR CONSEQUENCES

© 2020 K.A. Vasilenko[1], A.L. Zolkin[2], N.V. Abramov[3], D.O. Kurganov[3]

[1] Vladivostok State University of Economics and Service, Vladivostok, Russia
[2] Specialized production center of the Mid-Volga region, Samara, Russia
[3]Far Eastern Federal University, Vladivostok, Russia

The article is dedicated to the study of the problems related to hazard from malicious software in computer networks, such as DDOS attacks. Features of this software as well as method of defense against it have been reviewed in this article. It shall be noted that today the global Internet network is no longer considered as a fully safe information field for its users, due to the fact that modern anti-virus software is not aligned with a speed of modernization of new malicious software and cannot catch up malicious software, attack and hack methods in terms of development. Today the attacker uses the workstation of a basic user to take advantage of an attack on a bigger informational “cyber victim”. It is necessary to create a protective method against malicious software attacks in advance at the stage of malicious software development taking into account these circumstances.

Key words: computer networks, web server, malicious software, DDOS attacks, information, cyber security.