2. Baranov A. P. *Aktualnye problemy v sfere obespecheniya informatsionnoy bezopasnosti programmnogo obespecheniya* [Actual problems in the field of ensuring information security of software]. Available at: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/12ccdaa5fd89de1fc32575bd003e2eb1.

3. Dagaev A. F., Samoylov A. N., Borisova Ye. A. *Obespechenie informatsionnoy bezopasnosti v vychislitelnoy seti predpriyatiya* [Ensuring information security in the enterprise's computer network]. Available at: https://cyberleninka.ru/article/v/obespechenie-informatsionnoy-bezopasnosti-v-vychislitelnoy-seti-predpriyatiya.

4. Devyatin P. N. O probleme predstavleniya formalnoy modeli politiki bezopasnosti operatsionnykh sistem [On the problem of presenting a formal model of the security policy of operating systems]. *Trudy Instituta sistemnogo programmirovaniya RAN* [Works of the Institute for System Programming of the RAS], 2017, vol. 29, no. 3, pp. 7–14.

5. Dorofeev A. V., Markov A. S. Menedzhment informatsionnoy bezopasnosti: osnovnye kontseptsii [Management of Information Security: Basic Concepts]. *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2014, no. 1 (2), pp. 67–72.

6. Dunin V. S., Khokhlov N. S. Model ugroz informatsionnoy bezopasnosti kompleksnoy avtomatizirovannoy intellektualnoy sistemy “Bezopasnyy gorod” [The Model of Information Security Threats of the Integrated Automated Intelligent System “Safe City”]. *Vestnik Voronezhskogo instituta MVD Rossii* [Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia], 2011, no. 4, pp. 1–5.

7. Kodzheshau M. A. Tekhnologii i algoritmy informatsionnoy bezopasnosti [Technologies and algorithms for information security]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4 "Yestestvenno-matematicheskie i tekhnicheskie nauki"* [Bulletin of Adyghe State University. Series 4 "Natural-mathematical and technical sciences"], 2017, no. 2 (201), pp. 129–132.

8. Medvedev N. V., Grishin G. A. Modeli upravleniya dostupom v raspredelennykh informatsionnykh sistemakh [Access control models in distributed information systems]. *Mashinostroenie i kompyuternye tekhnologii* [Mechanical Engineering and Computer Technologies], 2011, no. 1, pp. 1–19.

9. Oladko A. Yu. Podsistema monitoringa i audita informatsionnoy bezopasnosti v operatsionnoy sisteme Linux [Subsystem of monitoring and auditing information security in the Linux operating system]. *Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskie nauki* [News of the Southern Federal University. Technical science], 2012, no. 12, pp. 22–28.

10. Rukasueva S. Yu., Bagaeva A. P. Windows i alternativnye ey operatsionnye sistemy [Windows and operating systems alternative to it]. *Aktualnye problemy aviatsii i kosmonavtiki* [Actual problems of aviation and cosmonautics], 2011, vol. 1, no. 7, pp. 459–460.

11. Trubachev Ye. S. Problemy informatsionnoy bezopasnosti. Metody i sredstva zashchity informatsionnykh resursov [Problems of information security. Methods and means of protection of information resources]. *Vestnik Volzhskogo universiteta imeni V.N. Tatishcheva* [Bulletin of Volzhsky University named after V.N. Tatishchev], 2009, no. 14, pp. 1–7.

12. Shubin A. N. Otsenka svoystv informatsionnykh sistem v standartakh po informatsionnoy bezopasnosti [Estimation of the properties of information systems in the standards of information security]. *Izvestiya Tulskogo gosudarstvennogo universiteta. Tekhnicheskie nauki* [News of Tula State University. Technical Science], 2013, vol. 3, pp. 336–345.

13. George K. Thiruvathukal. What's in an Algorithm? *Computing in Science & Engineering*, 2013, vol. 15, pp. 15–27.

14. Arne Johanson, Wilhelm Hasselbring. Software Engineering for Computational Science: Past, Present, Future. *Computing in Science & Engineering*, 2018, vol. 20, pp. 90–112.

УДК 004.032.26

ИДЕНТИФИКАЦИЯ DDOS-АТАК НА WEB-СЕРВЕРЫ

Статья поступила в редакцию 01.03.2019, в окончательном варианте – 08.04.2019.

Власенко Александра Владимировна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

кандидат технических наук, заведующая кафедрой компьютерных технологий и информационной безопасности Института информационных технологий и безопасности, e-mail: Vlasenko@kubstu.ru

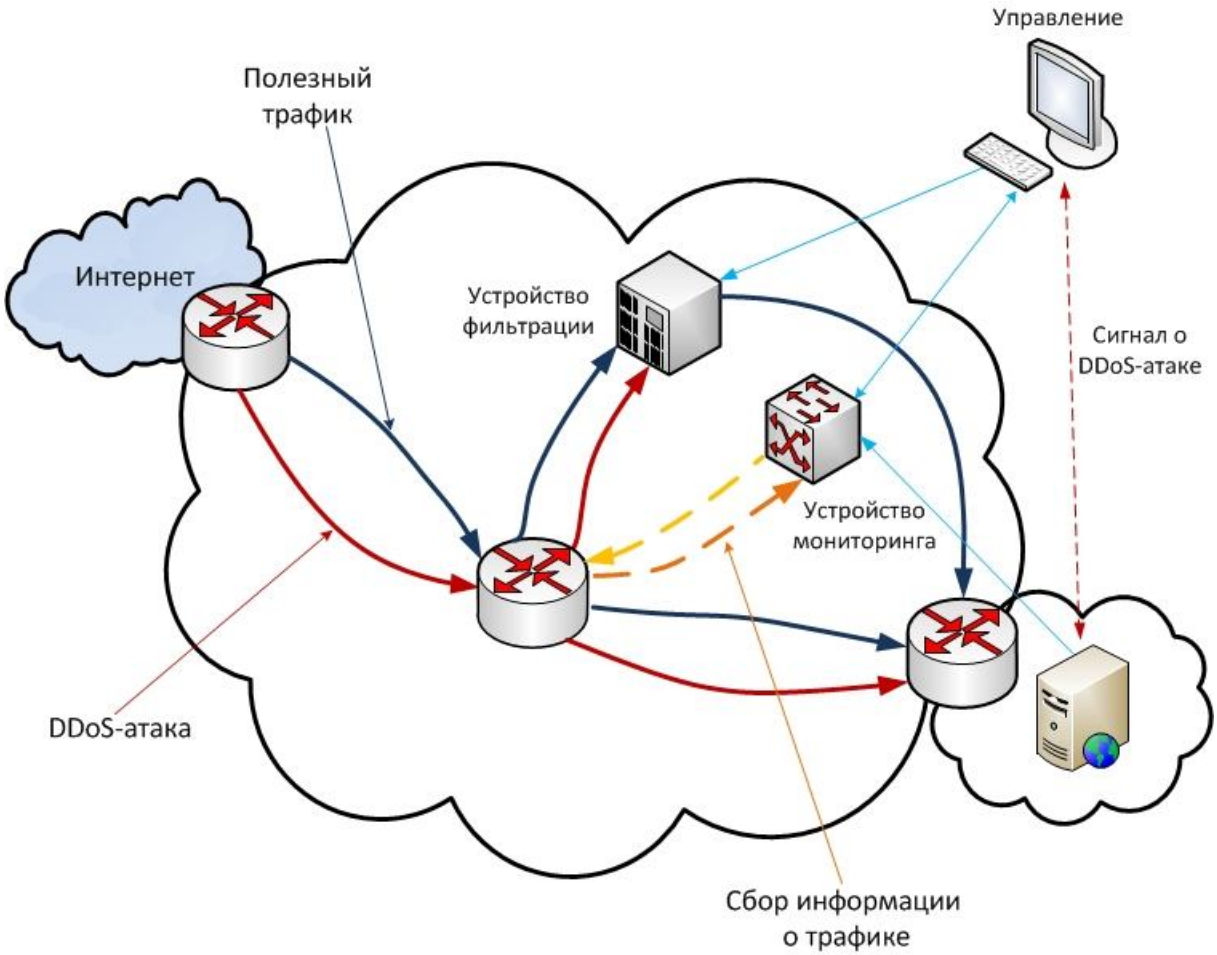
Дзьобан Павел Игоревич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2.

кандидат технических наук, старший преподаватель, Краснодар, e-mail: antiemoboy@mail.ru

В настоящее время жизнь обычного человека связана с активным использованием всевозможных онлайн-сервисов. Они помогают не только повысить скорость получения услуг, но и улучшить качество жизни. За комфорт принято платить, поэтому актуальность вопросов обеспечения безопасности оказания онлайн-услуг не вызывает сомнений. Невозможность использования сервисов может приводить к моральному ущербу и в некоторых случаях к существенным материальным потерям. Одним из возможных нарушений нормальной работы web-сервера могут быть атаки типа DOS/DDOS. В данной статье предлагается механизм обнаружения DDOS-атак. Для уменьшения трудоемкости обнаружения вторжений предлагается производить автоматизированный контроль состояния защищенности информационно-телекоммуникационных ресурсов, выполняя на постоянной основе комплекс следующих мероприятий: а) анализ log-файлов web-сервера (в работе рассмотрен пример сервера Apache); б) выявление различных параметров из необработанных запросов (используется для распознавания входящего запроса на web-сервер как «разрешенного» и «вредоносного»); в) проверка каждого входящего запроса (его параметров) к web-серверу по коррелированности с идентифицированными параметрами из log-файлов. Этот этап и приводит к выявлению вредоносного запроса к web-серверу, который делает возможной потенциальную DDOS-атаку.

Ключевые слова: протокол, отказ в обслуживании (DOS), распределенный отказ в обслуживании (DDOS), IP-спуфинг, log-файлы, flood, web-серверы, информационная безопасность

Графическая аннотация (Graphical annotation)



IDENTIFICATION OF DDOS ATTACKS ON WEB SERVERS

The article was received by editorial board on 01.03.2019, in the final version – 08.04.2019.

Vlasenko Alexandra V., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci. (Engineering), Head of the Department of Computer Technologies and Information Security of the Institute of Information Technology and Security, e-mail: Vlasenko@kubstu.ru

Dzoban Pavel I., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci. (Engineering), Senior Lecturer, e-mail: antiemoboy@mail.ru

Currently, the life of an ordinary person is associated with all kinds of online services that help not only to increase the speed of obtaining services, but also to the quality of life. It is accepted to pay for comfort and the relevance of the security issues of online services is not in doubt. Inability to use the service leads to moral damage and in some cases to significant material losses. One of the possible violations of the usual work of the web-server can be DOS/DDOS attacks. This scientific article proposes a mechanism for detecting DDOS attacks. To reduce the complexity of intrusion detection, it is proposed to carry out automated monitoring of the state of security of information and telecommunication resources, carrying out on a permanent basis a set of the following activities: a) the analysis of the log files of the web server (an example of the Apache server); b) detection of various parameters from unprocessed requests (used to recognize an incoming request to the web server as “allowed” and “malicious”); c) check each incoming request (its parameters) to the web-server by correlation with the identified parameters from the log files. This stage leads to the detection of a malicious request to the web server, which makes possible a potential DDOS attack.

Key words: protocol, denial of service (DOS), distributed denial of service (DDOS), IP spoofing, log files, flood, web servers, information security

Введение. Увеличивающийся темп развития информационно-телекоммуникационных технологий привел к росту числа предоставляемых гражданам онлайн-сервисов, что в свою очередь увеличило количество пользователей данных сервисов. Очевидно, что с помощью онлайн-сервисов человек становится значительно коммуникабельнее, выполняя в онлайн-режимах следующее: оплату счетов, покупки, общение с друзьями и семьей, поиск в интернете информации по различным темам, событиям, конференциям (серфинг) и т.д. Жизнь людей стала проще и качественнее, но зависима от работоспособности и функциональности программных, аппаратных средств и линий связи. Серьезную угрозу для национальной безопасности представляют атаки на информационные ресурсы, находящиеся в интернете, сервисы, обеспечивающие доступ к таким ресурсам. При нарушении работы хотя бы одного из составляющих использование привычных сервисов становится затруднительно и нередко ведет не только к моральному ущербу, но и к материальным потерям.

Одним из видов кибератак, которые направлены на сервера, являются атаки типа DDOS – англ. distributed denied of service, распределённая атака типа «отказ в обслуживании». Взаимосвязанные системы, такие как сервер базы данных, web-сервер, сервер облачных вычислений и т.д., постоянно находятся под угрозой вредоносных воздействий со стороны злоумышленников. Влияние на состояние безопасности таких систем не лежит в компетенции обычного пользователя онлайн-сервиса. Предоставление услуг в случае успешной атаки прекращается, онлайн-сервис становится недоступным для огромной аудитории пользователей. Одной из самых последних форм DDOS-атак является атака по протоколу http.

Обнаружение http-атаки после выполнения DDOS довольно сложная задача, она легко проходит первую линию защиты, такую как брандмауэр (межсетевой экран), IDS и т.д. Для обнаружения атак и предотвращения вторжений предложено много методов, однако все они трудоемки, так как необходимо исследовать и закрывать каждую уязвимость сети.

Несмотря на актуальность данной темы, некоторые ее аспекты остаются исследованными в литературе недостаточно полно. Поэтому целью настоящей статьи было устранение соответствующих недочетов, создание алгоритма идентификации DDOS-атак на web-серверы провайдеров онлайн-сервисов.

Виды DDOS-атак. Атаки типа DOS представляют собой кибератаки, где преступник стремится сделать машину или сетевой ресурс недоступным для предполагаемых пользователей временно или на неопределенный срок. При этом нарушается режим предоставления услуги из-за переполнения канала связи. Это достигается путем поступления от зараженного хоста огромного количества запросов к web-ресурсу с целью «перегрузить» канал связи или систему. В результате атаки сервер рано или поздно перестает успевать обрабатывать поступающие запросы и утрачивает работоспособность.

Атаки типа DDOS представляют собой кибератаки, которые достигают той же цели, но путем использования нескольких скомпрометированных машин пользователей.

DDOS-атака является достаточно распространенной формой воздействия на компьютерные сети. Она приводит к ряду проблем для пользователей сайтов, их владельцев, поставщиков услуг доступа к интернету (интернет-провайдеров).

На рисунке 1 представлена типовая схема реализации DDOS-атак.

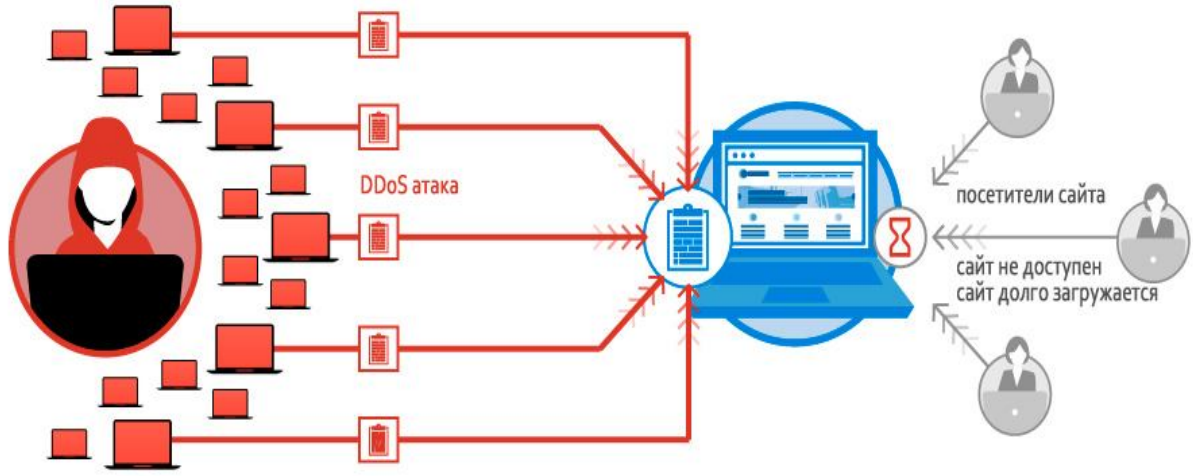


Рисунок 1 – Типовая схема реализации DDOS-атаки

Для начала необходимо рассмотреть виды DDOS-атак.

1. Прямые атаки. На один web-ресурс направляются запросы, отправленные с большого количества зараженных машин пользователей, – при этом промежуточная машина/машины не используется/не используются. Этот тип атаки может распространяться:

- на сетевом уровне (воздействие на сетевом уровне, такой как поток TCP, поток SYN, поток UDP и «ICMP-flood»);
- на уровне приложений (атака, переходящая в прикладной уровень, такой как «HTTP-flood», «FTP-flood» и т.д.)

2. Отраженные атаки. Зараженные машины пользователей сначала отправляют пакеты на некий «отражатель», чтобы подделать IP-адреса источников поступающих запросов.

Типы DDOS-атак в отношении технологий их реализации.

DDOS-атаки можно классифицировать по следующим типам.

1. Объемные атаки, использующие потоки UDP, ICMP и другие поддельные пакеты. Целью такого типа атаки является перегрузка полосы пропускания к web-ресурсу. Характеристикой интенсивности атаки объемного типа будет количество бит в секунду (суммарно, по всем поступающим сообщениям).

2. Протокольные атаки. Они используют потоки SYN, атаки фрагментированных пакетов, «Ping», «Smurf DDoS» и др. Этот тип атаки потребляет реальные ресурсы сервера или ресурсы промежуточного уровня – коммуникационного оборудования, включая межсетевые экраны и шлюзы. Характеристикой интенсивности атаки протокольного типа будет количество приходящих пакетов в секунду.

3. Атаки прикладного уровня. Они используют «длинные и медленные» атаки по GET/POST-запросам, целью которых являются уязвимости Apache, Windows или Open BSD и другого программного обеспечения. Собственно атака состоит из большого количества легитимных запросов, целью выполнения которых является создание сбоя web-сервера. Характеристикой интенсивности атаки прикладного уровня будет количество приходящих запросов в секунду.

4. Атака «UDP-flood». Как видно из названия, зараженные машины направляют огромное количество UDP-пакетов в адрес web-сервера. При этом злоумышленник отправляет большое количество пакетов UDP на случайные порты удаленной машины. Чрезмерный возврат ICMP-пакетов служит признаком выхода из строя web-сервера.

5. Атака «ICMP-flood». Зараженные машины направляют эхо-запросы ICMP-пакетов. Сервер предоставляет ответный ICMP-пакет, таким образом постепенно занижая пропускную способность канала.

6. Атака «SYN-flood» использует уязвимость в трехстороннем рукопожатии (handshaking) с протоколом TCP. В трехстороннем рукопожатии пакеты SYN сначала отправляются для соединения с хостом. Затем хост-получатель отвечает с ACK-пакетом, если он принимает решение о соединении с хостом-инициатором. Теперь в ответ на ACK-пакет первой машины необходимо отправить пакет ACK + SYN для установления соединения. В рамках использования этой атаки злоумышленник отправляет множественный запрос SYN через зараженный хост, используя его IP-адрес, с тем, чтобы ответ не доходил до источника.

7. Атака «Ping of death». Она представляет собой тип сетевой атаки, при которой web-сервер получает особым образом подделанный эхо-запрос (ping), после которого он перестает отвечать на запросы вообще. Максимально допустимый размер пакета составляет 65 535 байт. Для реализации данного типа атак злоумышленник отправляет пакеты «ping» с размером больше максимально допустимого предела. Это может привести к переполнению буфера памяти, выделенного для пакетов, и, в свою очередь, вызывать отказ в обслуживании для легитимных пакетов.

8. Атака «HTTP-flood». Она представляет собой легитимные GET или POST-запросы, используемые для атаки на web-сервер или web-приложение. В атаках «HTTP-flood» не используются искаженные пакеты, спуфинг или отражение метода. Поэтому требуется значительно меньшая пропускная способность, чем для реализации других типов атак. Данный тип атак считается одним из самых «эффективных», так как требует «выделения» максимального ресурса от web-сервера или web-приложение ресурса, на который выполняется атака.

9. Особое внимание следует уделить IP-спуфингу. Этот метод используется для создания IP-пакета с ложным IP-адресом, чтобы скрыть «личность пользователя». Подмена IP-адреса является одним из наиболее часто используемых фальсификаций для таких методов атаки. При реализации атак злоумышленник отправляет IP-пакеты с адресом источника скомпрометированной машины в сети, от имени которой и будут выполняться различные вредоносные сценарии. IP-спуфинг также активно используется злоумышленниками для обхода механизмов аутентификации пользователей.

Характеристика предлагаемого метода обнаружения DDOS-атак. В данной научной статье предлагается механизм обнаружения DDOS-атак. Опишем его отдельные этапы.

1. Для начала необходимо провести анализ log-файлов web-сервера, чтобы определить различные параметры, которые могут использоваться для определения потенциальной DDOS-атаки на web-сервер.

2. Затем необходимо использовать фильтр с идентификацией основных параметров. Ими являются: подозрительные IP-адреса; значение счетчика запросов с IP-адресов; скорость перехода по различ-

ным URL-адресам; среднее время пребывания на каждой web-странице; отметка времени запроса каждого источника; показатели полосы пропускания.

3. Проверка входящих запросов http для каждого входящего запроса на web-сервер. Вывод корреляции между полученным запросом и пороговым значением параметров, определенных в результате анализа log-файлов. Если для какого-либо запроса значения параметров превышают пороговое значение, то необходимо классифицировать такие запросы как вредоносные и блокировать IP-адрес источника.

Понятно, что при выполнении анализа по п. 3 в автоматическом режиме могут допускаться ошибки как 1-го, так и 2-го родов.

4. По выработанным правилам корреляции, подвергая анализу каждый запрос к web-ресурсу, определить IP-адреса потенциальных источников DDOS-атак, скомпрометированные и зараженные хосты.

Приводимые ниже примеры носят иллюстративный характер. По соображениям информационной безопасности конкретный адрес веб-ресурса, в отношении которого дана информация, не указывается.

На рисунке 2 приведен пример выполнения анализа log-файлов web-сервера с целью определения различных параметров, которые могут быть использованы для выявления потенциальной DDOS-атаки.

199.30.24.152	4/4/2015 2:19:14 PM	GET /images/item-separator.png HTTP/1.1	200	139	United States	http://iannet.org/
199.30.24.152	4/4/2015 2:19:14 PM	GET /iannet_logo.swf HTTP/1.1	200	1658	United States	http://iannet.org/iannet_logo.swf
157.55.39.71	4/4/2015 2:19:15 PM	GET /robots.txt HTTP/1.1	200	422	United States	-
202.46.54.43	4/4/2015 2:19:38 PM	HEAD /apps/SiteVerify/ HTTP/1.1	200	0	China	-
202.46.49.12	4/4/2015 2:19:39 PM	GET /apps/SiteVerify/ HTTP/1.1	200	4302	China	-
202.46.62.24	4/4/2015 2:19:40 PM	HEAD /apps/download.php?new=1 HTTP/1.1	404	0	China	http://www.iannet.org/apps/SiteVerif
202.46.53.68	4/4/2015 2:19:41 PM	GET /apps/download.php?new=1 HTTP/1.1	404	215	China	http://www.iannet.org/apps/SiteVerif
202.46.52.25	4/4/2015 2:19:42 PM	HEAD /apps/SiteVerify/download.php?new=1 HTTP/1.1	302	0	China	http://www.iannet.org/apps/SiteVerif
202.46.52.25	4/4/2015 2:19:42 PM	HEAD /apps/SiteVerify/siteverify.zip HTTP/1.1	200	0	China	http://www.iannet.org/apps/SiteVerif
191.236.33.18	4/4/2015 2:19:50 PM	GET / HTTP/1.1	200	15947	United States	-
36.76.244.171	4/4/2015 2:20:13 PM	GET /apps/TunnelBrokerUpdate/currentver.php?v=1,14 HTTP/1.1	200	4	Indonesia	-
180.76.5.72	4/4/2015 2:20:28 PM	GET /apps/GenerateHtPassWd HTTP/1.1	301	253	China	-
180.76.5.148	4/4/2015 2:20:29 PM	GET /apps/GenerateHtPassWd/ HTTP/1.1	200	2646	China	-

Рисунок 2 – Анализ log-файлов web-сервера. Примечание: красным цветом показано обращение по необходимому порту

Ниже представлены различные параметры, определенные в результате анализа log-файлов web-сервера Apache, вместе с их значениями для различных запросов. На рисунке 3 показана статистика посещений web-ресурса в зависимости от времени.

Рисунок 3 – Статистика по количеству посещений web-ресурса

На рисунке 4 представлена статистика в отношении ежедневного доступа к файлам по запросам пользователей.

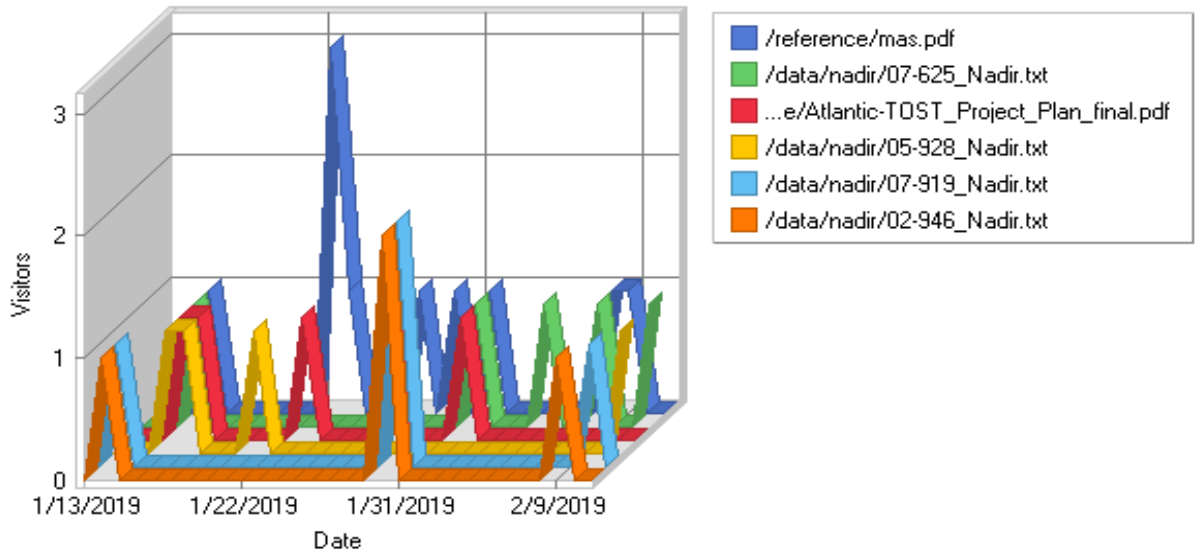


Рисунок 4 – Статистика обработки запросов пользователей

С использованием совокупности параметров, определенных в результате анализа log-файлов web-сервера Apache, необходимо проанализировать каждый входящий запрос к web-серверу. В результате сравнения пороговых показателей и фактических были выработаны правила корреляции для определения вредоносного потенциала DDOS-атак в каждом запросе.

Заключение. DDOS-атаки являются одной из главных проблем современных систем безопасности. Они могут привести к сбою web-сервера и вызвать серьезный ущерб бизнесу и репутации организации.

В данной статье предложен алгоритм выявления DDOS-атаки, который может быть реализован в автоматическом режиме.

На практике важен не только сам факт обнаружения атак типа DDOS, но и комплекс принятых мер, направленных на устранение выявленных уязвимостей в системе информационной безопасности интернет-ресурса.

Библиографический список

1. Брумштейн Ю. М. Надежность и качество информационных систем: анализ состава влияющих факторов с позиций информационной безопасности / Ю. М. Брумштейн, О. М. Князева, И. А. Дюдиков, Е. Ю. Васьковский // Надежность и качество : в 2 т. / под ред. Н. К. Юркова. – Пенза : Пензенский гос. ун-т, 2016. – Т. 1. – С. 101–106.

2. Бекенева Я. А. Анализ актуальных типов DDOS-атак и методов защиты от них / Я. А. Бекенева // Известия Санкт-Петербургского государственного электротехнического ниверситета «ЛЭТИ» им. В.И. Ульянова (Ленина). – 2016. – № 1. – С. 7–14.

3. Васьковский Е. Ю. Системный анализ функциональных возможностей счетчиков посещаемости сайтов / Е. Ю. Васьковский, Ю. М. Брумштейн // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 3 (31). – С. 45–58.

4. Власенко А. В. Анализ уязвимостей и моделирование атак на данные трафика «https» / А. В. Власенко, П. И. Дзьобан // Вестник Адыгейского государственного университета. Сер. 4. Естественно-математические и технические науки. – 2017. – № 2 (201). – С. 109–115.

5. Власенко А. В. Разработка и системный анализ математической модели угроз, модели нарушителя, процедур защиты Web-приложений на всех этапах функционирования / А. В. Власенко, П. И. Дзьобан // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2014. – № 101. – С. 2154–2164.

6. Свидетельство о государственной регистрации программы для ЭВМ № 2018618364. Программная среда криптографических преобразований / П. И. Дзьобан, А. В. Власенко, Б. В. Леваньков. – Зарегистрировано в реестре баз данных 11.06.2018.

7. Отчет «Лаборатории Касперского» о спаме и фишинге. – Режим доступа: https://threatpost.ru/new-report-on-spam-phishing-by-kasperskylab/29036/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.12.2018).

8. Паршин Г. К. DDOS-атаки и современные подходы к защите / Г. К. Паршин // Студенческий научный форум. – Режим доступа: https://scienceforum.ru/2017/article/2017029664, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 01.03.2019).

9. Терновой О. С. Раннее обнаружение DDOS-атак статистическими методами при учете сезонности / О. С. Терновой, А. С. Шатохин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012, июнь. – № 1 (25), ч. 1. – С. 104–112.

10. Фленов М. Е. Компьютер глазами хакера / М. Е. Фленов. – Санкт-Петербург : БХВ-Петербург, 2015.

11. Умницын М. Ю. Отслеживание состояния информационной системы на основе анализа данных о собы-

тиях / М. Ю. Умницын, С. В. Михальченко // Прикаспийский журнал: управление и высокие технологии. – 2017. – № 4 (40). – С. 165–173.

12. Хохлов Р. В. Противодействие DDOS-атакам с помощью Анти-DDOS / Р. В. Хохлов, С. А. Мишин, Р. А. Солодуха // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2017. – № 1. – С. 151–156.

13. Feinstein L. Statistical approaches to DDoS attack Detection and response / L. Feinstein, D. Schnackenberg, R. Balupari, D. Kindred // Proc. of DARPA Information Survivability Conference and Exposition. – 2013.

14. Protection Against DDoS and Data Modification Attack in Computational Grid Cluster Environment // I. J. Computer Network and Information Security. – 2017. – Vol. 7. – P. 12–18.

References

1. Brumshteyn Yu. M., Knyazeva O. M., Dyudikov I. A., Vaskovskiy Ye. Yu. Nadezhnost i kachestvo informatsionnykh sistem: analiz sostava vliyayushchikh faktorov s pozitsiy informatsionnoy bezopasnosti [Reliability and quality of information systems: analysis of the composition of influencing factors from the standpoint of information security]. *Nadezhnost i kachestvo: v 2 tomakh* [Reliability and Quality : in 2 volumes]. Ed. by N. K. Yurkov. Penza, Penza State University Publ., 2016, vol. 1, pp. 101–106.

2. Bekeneva Ya. A. Analiz aktualnykh tipov DDOS-atak i metodov zashchity ot nikh [Analysis of the actual types of DDOS attacks and methods of protection against them]. *Izvestiya Sankt-Peterburgskogo gosudarstvennogo elektrotekhnicheskogo niversiteta "LETI" im. V.I. Ulyanova (Lenina)* [News of the St. Petersburg State Electrotechnical Niversitet “LETI” them. V. I. Ulyanova (Lenin)], 2016, no. 1, pp. 7–14.

3. Vaskovskiy Ye. Yu., Brumshteyn Yu. M. Sistemnyy analiz funktsionalnykh vozmozhnostey schetchikov poseshchaemosti saytov [System analysis of the functionality of the site attendance counters]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Prikaspiysky Journal: Control and High Technologies], 2015, no. 3 (31), pp. 45–58.

4. Vlasenko A. V., Dzoban P. I. Analiz uyazvimostey i modelirovanie atak na dannye trafika "https" [Vulnerability analysis and modeling of attacks on “https” traffic data]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4 "Yestestvenno-matematicheskie i tekhnicheskie nauki"* [Bulletin of Adygeya State University. Series 4 "Natural-mathematical and technical sciences"], 2017, no. 2 (201), pp. 109–115.

5. Vlasenko A. V., Dzoban P. I. Razrabotka i sistemnyy analiz matematicheskoy modeli ugroz, modeli narushitelya, protsedur zashchity Web-prilozheniy na vsekh etapakh funktsionirovaniya [Development and system analysis of the mathematical model of threats, violator model, procedures for protecting Web applications at all stages of operation]. *Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta* [Polytematic network electronic scientific journal of the Kuban State Agrarian University], 2014, no. 101, pp. 2154–2164.

6. Dzioban P. I., Vlasenko A. V., Levankov B. V. *Certificate of state registration of computer program No. 2018618364. Software environment for cryptographic transformations*. Registered in the database registry 11.06.2018.

7. *Otchet "Laboratorii Kasperskogo" o spame i fishinge* [Kaspersky Lab report on spam and phishing]. Available at: https://threatpost.ru/new-report-on-spam-phishing-by-kasperskylab/29036/ (Accessed: 10.12.2018).

8. Parshin G. K. *DDOS-ataki i sovremennye podkhody k zashchite* [DDOS-attacks and modern approaches to protection]. Available at: https://scienceforum.ru/2017/article/2017029664 (Accessed: 01.03.2019).

9. Ternovoy O. S., Shatokhin A. S. Rannee obnaruzhenie DDOS-atak statisticheskimi metodami pri uchete sezonnosti [Early detection of DDOS-attacks by statistical methods with regard to seasonality]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of Tomsk State University of Control Systems and Radioelectronics], 2012, June, no. 1 (25), part 1, pp. 104–112.

10. Flenov M. Ye. *Kompyuter glazami khakera* [Computer as seen by a hacker]. St. Petersburg, BKhV-Petersburg Publ., 2015.

11. Umnitsyn M. Yu., Mikhalchenko S. V. Otslezhivanie sostoyaniya informatsionnoy sistemy na osnove analiza dannykh o sobytiyakh [Tracking the state of an information system based on the analysis of data on events]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Prikaspiysky Journal: Control and High Technologies], 2017, no. 4 (40), pp. 165–173.

12. Khokhlov R. V., Mishin S. A., Solodukha R. A. Protivodeystvie DDOS-atakam s pomoshchyu Anti-DDOS [Counter-measures of DDOS-attacks with the help of Anti-DDOS]. *Prestupnost v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy* [Crime in the field of information and telecommunication technologies: problems of prevention, disclosure and investigation of crimes], 2017, no. 1, pp. 151–156.

13. Feinstein L., Schnackenberg D., Balupari R., Kindred D. Statistical approaches to DDoS attack Detection and response. *Proc. of DARPA Information Survivability Conference and Exposition*, 2013.

14. Protection Against DDoS and Data Modification Attack in Computational Grid Cluster Environment. *I. J. Computer Network and Information Security*, 2017, vol. 7, pp. 12–18.