pISSN 2073-2872
eISSN 2311-875X

Угрозы и безопасность

ПРОГНОЗИРОВАНИЕ DDoS-АТАК ТИПА SYN НА WEB-РЕСУРСЫ*

София Сергеевна БАРМИНА[a,•], Фарида Муминджоновна ТАДЖИБАЕВА[b]

[a] студентка Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ, Казань, Российская Федерация
molibdenbora@yandex.ru
ORCID: отсутствует
SPIN-код: отсутствует

[b] студентка Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ, Казань, Российская Федерация
frida.t.1465@gmail.com
ORCID: отсутствует
SPIN-код: отсутствует

[•] Ответственный автор

История статьи:
Получена 24.07.2018
Получена в доработанном виде 16.08.2018
Одобрена 31.08.2018
Доступна онлайн 15.11.2018

УДК 004.056
JEL: C63, M15

Ключевые слова:
DDoS-атаки, SYN-флуд, прогнозирование, web-ресурсы, защита информации

Аннотация

Предмет. DoS – это хакерская атака на вычислительную систему, представляющая собой генерацию «мусорного» трафика с одного устройства (IP-адреса) на ресурс-жертву. Схема DoS – основа современных кибератак на отказ в обслуживании, при реализации которой не остается юридически значимых улик. DDoS-атаки осуществляются не с одного компьютера, а с нескольких компьютеров в сети.

Цели. Прогнозирование и исследование наиболее распространенного типа DDoS-атак – DDoS-атак длительностью до 4 часов и SYN-флуд атак, которые входят в топ-10 сетевых атак и приводят к серьезным сбоям в работе web-ресурсов.

Методология. В работе реализован корреляционный анализ временных рядов SYN-флуд атак и DDoS-атак длительностью до 4 часов, определены коэффициенты автокорреляции данных, индексы сезонности, кросс-корреляция рядов. Осуществлено прогнозирование SYN-флуд атак на будущие кварталы 2018 и 2019 гг. методом экспоненциального сглаживания.

Результаты. Установлено, что SYN-флуд атакам присуща сезонность: наибольшее количество атак ожидается в I и III кв. 2018 и 2019 гг. Для DDoS-атак длительностью до 4 часов также выявлена сезонность в I кв. календарного года, а значит, в I кв. 2019 г. следует ожидать наибольшее количество атак данной длительности. Согласно прогнозу, выполненному при помощи статистической модели экспоненциального сглаживания, в III и IV кв. 2018 г. доля таких атак должна составить по 59% в каждом. В I кв. 2019 г. ожидается 61% SYN-флуд атак, во II кв. – 57%.

Выводы. Выявлены корреляционные зависимости между SYN-флуд атаками и DDoS-атаками длительностью до 4 часов, показана сезонность данных атак. Сделан прогноз по SYN-флуд атакам на конец 2018 и начало 2019 г. Эти данные позволяют подготовиться к ожидаемому количеству SYN-флуд атак на web-ресурсы и выработать меры предосторожности.

Для цитирования: Бармина С.С., Таджибаева Ф.М. Прогнозирование DDoS-атак типа SYN на web-ресурсы // Национальные интересы: приоритеты и безопасность. – 2018. – Т. 14, № 11. – С. 2162 – 2174.
https://doi.org/10.24891/ni.14.11.2162

Введение

DDoS-атаки можно классифицировать по протоколам. В России их чаще всего подразделяют на три большие группы: UDP (*User Datagram Protocol*), TCP (*Transmission Control Protocol*), прочие. Такая классификация считается упрощенной и базируется на основных протоколах, которые используют для передачи данных в сети [1, 2].

Уязвимости данных протоколов позволяют хакерам производить атаки[1]. UDP и TCP используются чаще, поэтому атаки с их использованием выделяют в отдельные группы. Категория «прочие» включает в себя атаки на такие протоколы как: ICMP, GRE, IPIP, ESP, AH, SCTP, OSPF, SWIPE, TLSP, Compaq_PEE и т.д. На западе можно встретить иное разделение, в котором выделяют пять типов DDoS-атак: TCP, HTTP, UDP, ICMP и др.[2] [3–6].

Подобное разделение позволяет выявлять тенденции, а именно: какие протоколы в большей степени подвергаются паразитному трафику, а какие – в меньшей. На основе этих тенденций корректируются стратегии защиты web-ресурсов, разрабатываются новые алгоритмы фильтрации паразитного трафика [7–13].

По механизму воздействия можно выделить три группы атак типа «отказ в обслуживании». Первая группа – это атаки, направленные на переполнение канала связи, то есть различные типы флуда. Флуд используется в целях создания мощного потока запросов (пакетов данных), который займет собой всю выделенную ресурсу-жертве полосу трафика. Данные атаки воздействуют на канальный уровень модели OSI. Вторая группа атак использует уязвимости стека сетевых протоколов, воздействуя на сетевой и транспортный уровни модели OSI. Третья группа – это DDoS-атаки, ориентированные на прикладной уровень модели OSI. Топ-5 атак каждой группы представлен на *рис. 1*.

По данным исследований «Лаборатории Касперского», с 2016 г. большую часть DDoS-атак составляют атаки типа SYN (от 54 до 82% ежеквартально), а наиболее распространенными по длительности являются DDoS-атаки длительностью до 4 ч включительно (от 59 до 86% ежеквартально).

DDoS-атаки типа SYN (или SYN flood-атаки) – атаки, использующие уязвимости стека сетевых протоколов. Во время SYN-флуда на атакуемый сервер с большой скоростью посылаются SYN-запросы, содержащие поддельный IP-адрес источника. SYN-флуд поражает сервер, занимая всю память таблицы соединений (*Transmission Control Block, TCB*), которую используют для обработки и хранения входящих пакетов. Это вызывает критическое падение производительности и отказ в обслуживании – как следствие.

В данной работе будут построены и проанализированы временные ряды DDoS-атак типа SYN и DDoS-атак длительностью до 4 ч, на основе которых будет предложен прогноз DDoS-атак типа SYN на второе полугодие 2018 г., а также первое полугодие 2019 г.

Анализ временных рядов на основе статистических данных

Для анализа временных рядов статистические данные «Лаборатории Касперского» были сведены в *табл. 1*.

Выполним анализ временного ряда DDoS-атак типа SYN по следующему алгоритму:

1) проведем корреляционный анализ;

2) рассчитаем индекс сезонности.

[*] Авторы выражают благодарность и глубокую признательность д.т.н., доценту кафедры систем информационной безопасности ФГБ ОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ» Марине Владимировне ТУМБИНСКОЙ за советы и ценные замечания при работе над данной статьей.

[1] *Фролов С.Г., Демин А.Ю.* Типы DDoS-атак, методы профилактики и защиты от них: материалы III Международной научной конференции «Информационные технологии в науке, управлении, социальной сфере и медицине». Томск: Изд-во Национального исследовательского Томского политехнического ун-та, 2016. С. 76–78; *Дубровин Д.А.* Проблемы и перспективы развития систем защиты от DDoS-атак: материалы VI Международного научного студенческого конгресса «Гражданское общество России: становление и пути развития». М.: Изд-во Финансового ун-та при Правительстве Российской Федерации, 2015. С. 1683–1688; *Зеленский М.Д.* DDoS-атаки: типы атак, устранение DDoS-атак: материалы IV Всероссийской научно-технической конференции «Студенческая наука для развития информационного общества». Ставрополь: Изд-во Северо-Кавказского федерального ун-та, 2016. С. 241–243.

[2] *Керценбаум К.М.* Информационная безопасность, или просто о сложном // Право и кибербезопасность. 2012. № 1. С. 30–32.

Лаг автокорреляции определим, как $n/2$, где n – общее число периодов в исследовании, в данном случае $n = 9$. Значения автокорреляции временного ряда DDoS-атак типа SYN представлены в *табл. 2*.

Из данных *табл. 2* видно, что значение корреляции между последовательными значениями ряда невысокое, следовательно, тренд отсутствует. Корреляция между исходным рядом и сдвинутым на 5 позиций заметная – 0,6334. Следовательно, в данных присутствует сезонность и период сезонности равен 5 кварталам. Расчет и анализ индекса сезонности для DDoS-атак типа SYN представлен в *табл. 3*.

В случае если индекс сезонности превышает единицу, присутствует влияние сезонного фактора в сторону увеличения уровней динамического ряда, в противном случае сезонный фактор вызывает снижение уровней динамического ряда. Анализ показал, что в I и III кв. ожидается наибольшее количество DDoS-атак типа SYN.

Аналогично выполним анализ временного ряда DDoS-атак длительностью до 4 ч. Результаты автокорреляции приведены в *табл. 4*.

Из *табл. 4* видно, что значение корреляции между последовательными значениями ряда высокое, следовательно, тренд присутствует. Корреляция между исходным рядом и сдвинутым на 5 позиций умеренная – 0,4628. Следовательно, в данных может присутствовать сезонность. Рассчитаем и проанализируем индекс сезонности (*табл. 5*).

Анализ показал, что в I кв. следует ожидать максимального количества атак длительностью до 4 ч.

Для выявления корреляционной зависимости рассчитаем взаимную корреляционную функцию, допуская запаздывание длительности атак по отношению к количеству SYN-флуд атак. Результаты кросс-корреляции приведены в *табл. 6*.

Как видно из данных *табл. 6*, корреляционная связь между переменными ряда атак типа SYN и ряда длительности атак умеренно сильна при временном запаздывании на три квартала. Тенденция временных рядов с учетом лага в три квартала для временного ряда длительности атак представлена на *рис. 2*.

Корреляционный анализ показал, что временные ряды имеют схожую тенденцию. Связь между SYN-флуд атаками и атаками длительностью до 4 ч умеренно сильная, не критичная, прослеживается при запаздывании длительности на три временных лага (в нашем случае – три квартала).

Прогнозирование с помощью статистической модели экспоненциального сглаживания

Согласно модели экспоненциального сглаживания[3] [14, 15], каждое следующее значение ряда вычисляется согласно формуле:

$$y^*_{t+1} = \alpha\ y_t + (1 - \alpha\ )\, y^*_t,$$

где y^*_{t+1} – прогнозное значение;

α – параметр сглаживания;

y_t – текущее наблюдаемое значение;

y^*_t – прогнозное значение текущего значения (средняя взвешенная экспоненциальная за предшествующий период).

1. Определяем значение параметра сглаживания по формуле:

$$A = 2/(n + 1), \qquad (1)$$

[3] *Бажанов Н.Н.* Экспоненциальное сглаживание как метод прогнозирования временных рядов: материалы Международной научно-практической конференции «Теория и практика науки третьего тысячелетия». Уфа: Башкирский государственный университет, 2014. С. 194–196; *Войтишкина А.Л.* Применение метода экспоненциального сглаживания при среднесрочном прогнозировании бюджета: материалы Международной научно-практической конференции «Математическое моделирование в экономике, управлении и образовании». СПб: Эйдос, 2015. С. 19–27; *Тарджуманян А.А.* Прогнозирование по методам простого и двойного экспоненциального сглаживания // Молодежный научно-технический вестник. 2015. № 3. С. 39.

где n – число наблюдений, входящих в интервал сглаживания. В данном случае α = 0,2.

2. Определяем начальное значение y_0 двумя способами:

I способ (*среднее арифметическое*): y_0 = 62,44.

II способ (*принимаем первое значение базы прогноза*): y_0 = 54,9.

3. Рассчитаем экспоненциально взвешенную среднюю для каждого периода, используя формулу (1).

I способ:

$y_{\text{IIкв.2016}} = 54,9 \cdot 0,2 + (1 - 0,2) \cdot 62,44 = 60,932$

…

$y_{\text{Iкв.2018}} = 55,63 \cdot 0,2 + (1 - 0,2) \cdot 62,064 = 60,77.$

II способ:

$y_{\text{IIкв.2016}} = 54,9 \cdot 0,2 + (1 - 0,2) \cdot 54,9 = 54,9;$

…

$y_{\text{Iкв.2018}} = 55,63 \cdot 0,2 + (1 - 0,2) \cdot 60,48 = 59,71.$

4. По этой же формуле вычисляем прогнозное значение:

$y_{\text{IIкв.2018}} = 57,3 \cdot 0,2 + (1 - 0,2) \cdot 60,77 = 60,022$ (I способ);

$y_{\text{IIкв.2018}} = 57,3 \cdot 0,2 + (1 - 0,2) \cdot 59,51 = 59,068$ (II способ).

Результаты вычислений представлены в *табл. 7*.

5. Рассчитываем среднюю относительную ошибку по формуле:

$$\overline{\varepsilon} = \frac{1}{n} \cdot \sum_{i=1}^{n} \left[\frac{|y_{\text{н}} - y_{\text{р}}|}{y_{\text{н}}} \cdot 100 \right],$$

где $y_{\text{н}}$ – начальное значение, $y_{\text{р}}$ – расчетное значение;

$\overline{\varepsilon}$ = 151,36/9 = 16,82% (I способ);

$\overline{\varepsilon}$ = 114,47/9 = 12,72% (II способ).

Эмпирической мерой точности прогноза, служит величина его средней относительной ошибки. Интерпретация оценки точности (%): меньше 10 – высокая; ∈ [10; 20] – хорошая; ∈ [20; 50] – удовлетворительная; больше 50 – неудовлетворительная.

Согласно проведенным расчетам, в обоих случаях можно говорить о том, что точность прогноза хорошая. Однако следует заметить, что средняя относительная ошибка при вычислениях вторым способом меньше, следовательно, искомыми будем считать прогнозы по второму способу. Повторим вычисления для прогноза на III и IV кв. 2018 г., I и II кв. 2019 г.

Таким образом, во II кв. 2018 г. ожидается 59,07% DDoS-атак типа SYN, в III и IV кв. 2018 г. их количество составит по 59,12% в каждом. В I кв. 2019 г. ожидается 60,9% SYN-флуд атак, во II кв. 2019 года – 57,08%.

Таблица 1
Собранные данные о количестве DDoS-атак типа SYN и DDoS-атак длительностью до 4 ч

Table 1
Collected data on the number of SYN flood DDoS-attacks and DDoS-attacks lasting up to 4 hours

Год	Период	Доля DDoS-атак типа SYN, %	Доля DDoS-атак длительностью не более 4 часов, %
2016	I кв.	54,9	67,8
	II кв.	76	59,8
	III кв.	81,03	68,98
	IV кв.	75,33	67,42
2017	I кв.	48,07	82,21
	II кв.	53,26	85,93
	III кв.	60,4	76,09
	IV кв.	55,63	76,76
2018	I кв.	57,3	80,73

Источник: авторская разработка

Source: Authoring

Таблица 2
Автокорреляция для временного ряда DDoS-атак типа SYN

Table 2
Autocorrelation for time series of SYN flood DDoS-attacks

Лаг	Автокорреляция
x_0	1
x_1	0,3718
x_2	–0,2514
x_3	–0,4335
x_4	0,3907
x_5	0,6334

Источник: авторская разработка

Source: Authoring

Таблица 3
Индексы сезонности для DDoS-атак типа SYN

Table 3
Seasonal indices for SYN flood DDoS-attacks

Период	2016	2017	2018	Индекс сезонности
I кв.	54,9	48,07	57,3	1,1409
II кв.	76	53,26	–	0,9201
III кв.	81,03	60,4	–	1,0068
IV кв.	75,33	55,63	–	0,9322

Источник: авторская разработка

Source: Authoring

Таблица 4
Автокорреляция для временного ряда DDoS-атак длительностью до 4 ч

Table 4
Autocorrelation for time series of DDoS-attacks lasting up to 4 hours

Лаг	Автокорреляция
x_0	1
x_1	0,5502
x_2	0,2582
x_3	0,0101
x_4	–0,3254
x_5	0,4628

Источник: авторская разработка

Source: Authoring

Таблица 5
Индексы сезонности для DDoS-атак длительностью до 4 ч

Table 5
Seasonal indices for DDoS-attacks lasting up to 4 hours

Период	2016	2017	2018	Индекс сезонности
I кв.	67,8	82,21	80,73	1,3864
II кв.	59,8	85,93	...	0,8756
III кв.	68,98	76,09	...	0,8717
IV кв.	67,42	76,76	...	0,8663

Источник: авторская разработка

Source: Authoring

Таблица 6
Кросс-корреляция ряда атак типа SYN и ряда атак длительностью до 4 ч

Table 6
Cross-correlation of a number of SYN-flood attacks and a number of attacks lasting up to 4 hours

Лаг	Кросс-корреляция
x_0	–0,75855
x_1	–0,29303
x_2	0,28405
x_3	0,54873
x_4	–0,29211
x_5	–0,91739

Источник: авторская разработка

Source: Authoring

Таблица 7

Прогнозирование методом экспоненциального сглаживания

Table 7
Forecasting by the method of exponential smoothing

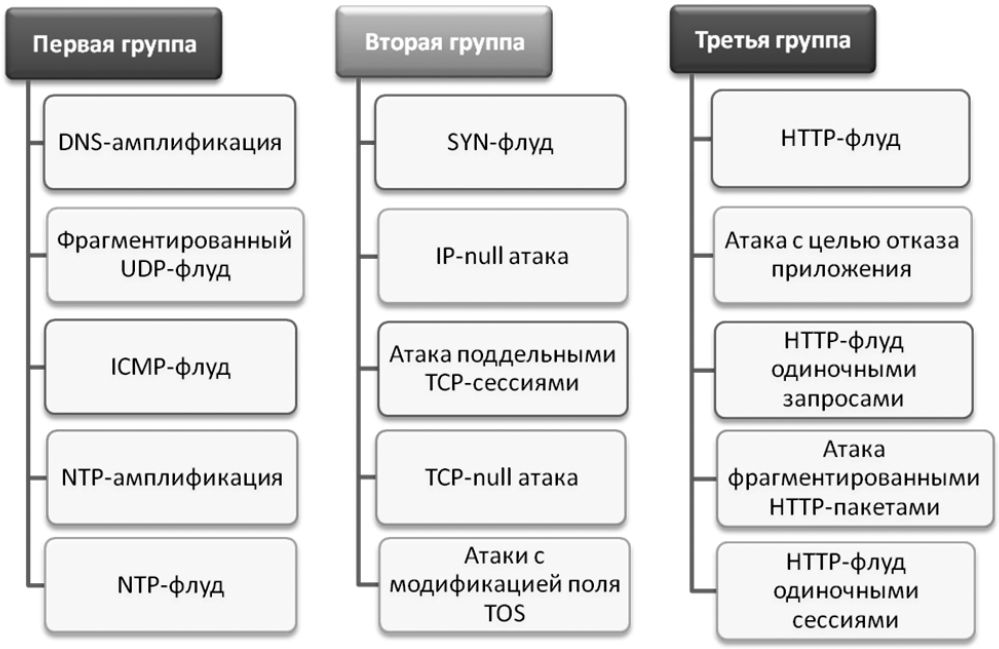
Период	Доля DDoS-атак типа SYN, %	Экспоненциально взвешенная средняя, y_t		Расчет средней относительной ошибки $\frac{\lvert y_н - y_р \rvert}{y_н} \cdot 100$, %	
		I способ	II способ	I способ	II способ
I кв. 2016 г.	54,9	62,44	54,9	13,73	–
II кв. 2016 г.	76	60,932	54,9	19,83	27,76
III кв. 2016 г.	81,03	63,95	59,12	21,07	27,04
IV кв. 2016 г.	75,33	67,366	63,502	10,57	15,7
I кв. 2017 г.	48,07	68,96	65,87	43,46	9,59
II кв. 2017 г.	53,26	64,782	62,31	21,63	21,64
III кв. 2017 г.	60,4	62,48	60,5	3,44	0,16
IV кв. 2017 г.	55,63	62,064	60,48	11,57	8,72
I кв. 2018 г.	57,3	60,77	59,51	6,06	3,86
Итого...				***151,36***	***114,47***
Прогноз на II кв. 2018 г.	…	60,022	59,068	…	…

Источник: авторская разработка

Source: Authoring

Рисунок 1
Топ-5 DDoS-атак в каждой группе механизма воздействия

Figure 1
Top-5 of DDoS attacks in each impact mechanism group

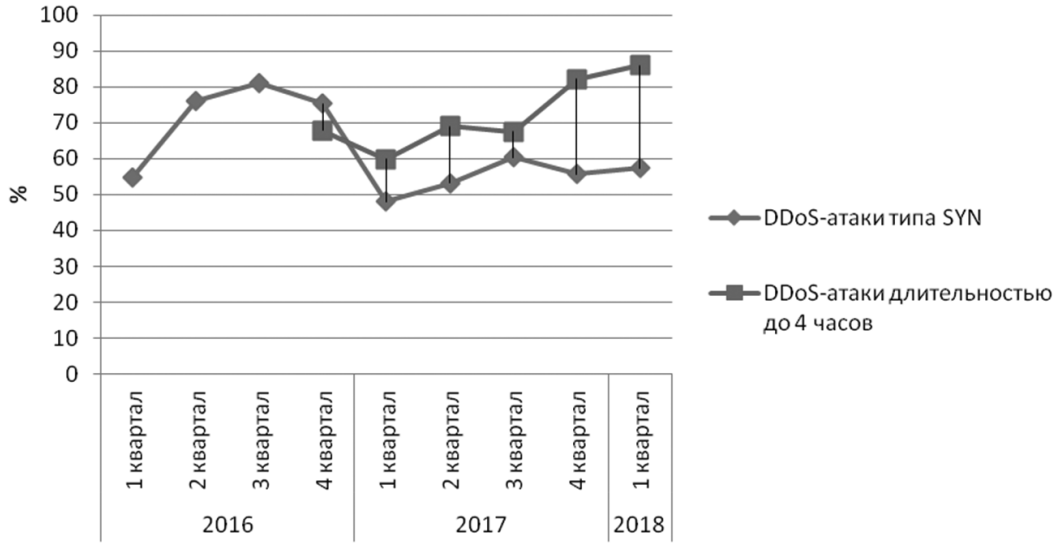


Источник: авторская разработка

Source: Authoring

Рисунок 2
Тенденция временных рядов с учетом лага

Figure 2
The trend of time series taking into account the lag



Источник: авторская разработка

Source: Authoring

Список литературы

1. *Харитонов В.С., Черяпкин Д.П.* DDoS-атака: классификация и особенности // Постулат. 2016. № 12. С. 45. URL: http://e-postulat.ru/index.php/Postulat/article/view/285/302
2. *Бондаренко М.С.* Обзор методов и инструментов для реализации распределенных атак отказа в обслуживании // Вестник Воронежского института высоких технологий. 2017. № 4. С. 59–63.
3. *Тумбинская М.В.* Организационное обеспечение процесса управления IT-инфраструктурой в системе защиты информации на предприятии // Национальные интересы: приоритеты и безопасность. 2015. № 1. С. 31–41. URL: https://cyberleninka.ru/article/v/organizatsionnoe-obespechenie-protsessa-upravleniya-it-infrastrukturoy-v-sisteme-zaschity-informatsii-na-predpriyatii
4. *Тумбинская М.В.* Модель защищенной информационной системы интернет-банкинга // Прикладная информатика. 2015. Т. 10. № 5. С. 62–72.
5. *Ревенков П.В., Бердюгин А.А.* Кибербезопасность в условиях Интернета вещей и электронного банкинга // Национальные интересы: приоритеты и безопасность. 2016. Т. 12. Вып. 11. С. 158–169. URL: https://cyberleninka.ru/article/v/kiberbezopasnost-v-usloviyah-interneta-veschey-i-elektronnogo-bankinga
6. *Чирков Д.К., Саркисян А.Ж.* Преступность в сфере высоких технологий: тенденции и перспективы // Вопросы безопасности. 2013. № 2. С. 160–181.
7. *Терентьев А.М.* Выбор адекватных средств информационной защиты персонального компьютера в России // Национальные интересы: приоритеты и безопасность. 2012. № 33. С. 37–42. URL: https://cyberleninka.ru/article/v/vybor-adekvatnyh-sredstv-informatsionnoy-zaschity-personalnogo-kompyutera-v-rossii
8. *Жуков Ю.В.* Основы веб-хакинга: нападение и защита. СПб.: Питер, 2012. 208 с.
9. *Бирюков А.А.* Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. 474 с.
10. *Шаньгин В.Ф.* Информационная безопасность и защита информации. М.: ДМК Пресс, 2014. 702 с.
11. *Листопад М.Е., Коротченко С.Е.* Совершенствование методики оценки системы информационной безопасности в России // Национальные интересы: приоритеты и безопасность. 2017. Т. 13. Вып. 6. С. 1162–1175. URL: https://doi.org/10.24891/ni.13.6.1162
12. *Жидко Е.А., Попова Л.Г.* Информационная безопасность модернизируемой России: постановка задачи // Информация и безопасность. 2011. № 2. С. 181–190.
13. *Зефиров С.Л.* Проблема измерения и оценивания информационной безопасности организации // Открытое образование. 2011. № 2-2. С. 134–137.
14. *Сапунов П.* Основы прогнозирования. Инновационные процессы и устойчивость национальной экономики. М.: Издательские решения, 2016. 50 с.

15. *Кузнецов Д.А.* Системно-информационные модели прогнозирования динамики развития экономических систем // Прикладная информатика. 2010. № 6. С. 3–9. URL: https://cyberleninka.ru/article/n/system-information-models-of-forecasting-of-dynamics-of-development-of-economic-systems

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

pISSN 2073-2872
eISSN 2311-875X

Threats and Security

FORECASTING SYN FLOOD DDoS ATTACKS ON WEB RESOURCES

Sof'ya S. BARMINA[a,•], Farida M. TADZHIBAEVA[b]

[a] Kazan National Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI), Kazan, Republic of Tatarstan, Russian Federation
molibdenbora@yandex.ru
ORCID: not available

[b] Kazan National Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI), Kazan, Republic of Tatarstan, Russian Federation
frida.t.1465@gmail.com
ORCID: not available

[•] Corresponding author

Article history:
Received 24 July 2018
Received in revised form
16 August 2018
Accepted 31 August 2018
Available online
15 November 2018

JEL classification: C63, M15

Keywords: DDoS attack, SYN flood, forecasting, web resource, information protection

Abstract

Subject Denial-of-service attacks are performed by hackers targeting the computer system. It is a basic scheme for cyberattacks undermining a service, which leaves no legally substantive evidence. DDoS attacks are effectuated through several computers.

Objectives The research is to forecast and examine the most common type of DDoS attacks lasting less than four hours and SYN flood attacks being on Top 10 of the internet attacks and causing serious breakdowns of web resources.

Methods The research is based on a correlation analysis of time series of SYN flood and DDoS attacks of four hours and less, cross-correlation of time series. We forecast SYN flood attacks for the coming quarters of 2018 and 2019 by the exponential smoothing method.

Results SYN floods are found to be of seasonal nature. DDoS attacks lasting less than four hours were also seasonal in Q1 of a calendar year, thereby making us expect more attacks in Q1 2019.

Conclusions and Relevance We traced a correlation between SYN flood attacks and DDoS attacks lasting less than four hours and showed their seasonality. The article provides the forecast of SYN flood attacks for the end of 2018 and beginning of 2019. The data allows for respective preparatory actions in order to protect web resources from SYN flood attacks.

Please cite this article as: Barmina S.S., Tadzhibaeva F.M. Forecasting SYN Flood DDoS Attacks on Web Resources. *National Interests: Priorities and Security*, 2018, vol. 14, iss. 11, pp. 2162–2174.
https://doi.org/10.24891/ni.14.11.2162

Acknowledgments

We express our gratitude and deep appreciation to Marina V. TUMBINSKAYA, Doctor of Engineering Science, Associate Professor of the Department for Information Security Systems of the Kazan National Research Technical University named after A.N. Tupolev – KAI, for the valuable advice and comments on the article.

References

1. Kharitonov V.S., Cheryapkin D.P. [DDoS attack: Classification and characteristics]. *Postulat*, 2016, no. 12, p. 45. (In Russ.) URL: http://e-postulat.ru/index.php/Postulat/article/view/285/302

2. Bondarenko M.S. [Overviewing methods and tools to perform DDoS attacks]. *Vestnik Voronezhskogo instituta vysokikh tekhnologii = Bulletin of Voronezh Institute of High Technologies*, 2017, no. 4, pp. 59–63. (In Russ.)

3. Tumbinskaya M.V. [Organizational support to IT infrastructure management in the information security system of an enterprise]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2015, no. 1, pp. 31–41. URL: https://cyberleninka.ru/article/v/organizatsionnoe-obespechenie-protsessa-upravleniya-it-infrastrukturoy-v-sisteme-zaschity-informatsii-na-predpriyatii (In Russ.)

4. Tumbinskaya M.V. [Secure information system model of Internet banking]. *Prikladnaya informatika = Applied Informatics*, 2015, vol. 10, no. 5, pp. 62–72. URL: https://cyberleninka.ru/article/v/model-zaschischennoy-informatsionnoy-sistemy-internet-bankinga (In Russ.)

5. Revenkov P.V., Berdyugin A.A. [Cybersecurity in the Internet of Things and electronic banking]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2016, vol. 12, iss. 11, pp. 158–169. URL: https://cyberleninka.ru/article/v/kiberbezopasnost-v-usloviyah-interneta-veschey-i-elektronnogo-bankinga (In Russ.)

6. Chirkov D.K., Sarkisyan A.Zh. [High technology crime: Tendencies and perspectives]. *Voprosy bezopasnosti = Security Issues*, 2013, no. 2, pp. 160–181. (In Russ.) URL: https://doi.org/10.7256/2306-0417.2013.2.608

7. Terent'ev A.M. [Choice of adequate information security software PC in Russia]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2012, no. 33, pp. 37–42. URL: https://cyberleninka.ru/article/v/vybor-adekvatnyh-sredstv-informatsionnoy-zaschity-personalnogo-kompyutera-v-rossii (In Russ.)

8. Zhukov Yu.V. *Osnovy veb-khakinga: napadenie i zashchita* [The basics of web hacking: attack and defense]. St. Petersburg, Piter Publ., 2012, 208 p.

9. Biryukov A.A. *Informatsionnaya bezopasnost': zashchita i napadenie* [Information security: protection and attack]. Moscow, DMK Press Publ., 2012, 474 p.

10. Shan'gin V.F. *Informatsionnaya bezopasnost' i zashchita informatsii* [Information security and information defense]. Moscow, DMK Press Publ., 2014, 702 p.

11. Listopad M.E., Korotchenko S.E. [Improving the method for evaluation of the information security system in Russia]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security,* 2017, vol. 13, iss. 6, pp. 1162–1175. URL: https://cyberleninka.ru/article/v/sovershenstvovanie-metodiki-otsenki-sistemy-informatsionnoy-bezopasnosti-v-rossii (In Russ.)

12. Zhidko E.A., Popova L.G. [Information security of Russia in modernization: Statement of the problem]. *Informatsiya i bezopasnost' = Information and Security*, 2011, no. 2, pp. 181–190. (In Russ.)

13. Zefirov S.L. [The problem of measuring and evaluating the information security of an organization]. *Otkrytoe obrazovanie = Open Education,* 2011, no. 2-2, pp. 134–137. (In Russ.)

14. Sapunov P. *Osnovy prognozirovaniya. Innovatsionnye protsessy i ustoichivost' natsional'noi ekonomiki* [Principles of forecasting. Innovative processes and sustainability of the national economy]. Moscow, Izdatel'skie resheniya Publ., 2016, 50 p.

15. Kuznetsov D.A. [System-information models of forecasting of dynamics of development of economic systems]. *Prikladnaya informatika = Applied Informatics,* 2010, no. 6, pp. 3–9. URL: https://cyberleninka.ru/article/n/system-information-models-of-forecasting-of-dynamics-of-development-of-economic-systems (In Russ.)

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.