

СТАТИСТИКА АТАК НА ВЕБ-ПРИЛОЖЕНИЯ

III КВАРТАЛ 2017 ГОДА

POSITIVE TECHNOLOGIES

СОДЕРЖАНИЕ

Введение..... 3

Основные результаты..... 4

Статистика атак на веб-приложения 5

 Типы атак..... 5

 Источники атак..... 12

 Динамика атак..... 12

Выводы 15

ВВЕДЕНИЕ

В данном исследовании представлена статистика атак на веб-приложения за III квартал 2017 года. Исходные данные были получены в ходе пилотных проектов по внедрению меж-сетевого экрана уровня приложений PT Application Firewall, а также по итогам работы PT AF для защиты веб-приложений компании Positive Technologies.

В отчете рассмотрены наиболее распространенные типы атак, цели атак, их источники, а также интенсивность и распределение во времени. Кроме того, приводится статистика по отдельным отраслям экономики. Исследование атак позволяет оценить текущие тенденции в области безопасности веб-приложений, выявить актуальные угрозы и выделить факторы, на которые прежде всего следует обратить внимание при разработке веб-приложения и построении системы защиты.

Для получения более достоверных результатов автоматизированный поиск уязвимостей с помощью специализированного ПО для сканирования веб-приложений (например, Acunetix) был исключен из исходных данных. Приведенные в отчете примеры атак были проверены вручную на предмет ложных срабатываний и являются достоверными.

Ресурсы Positive Technologies рассматриваются в совокупности с ресурсами компаний из сферы информационных технологий.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ



Практически каждая вторая атака

нацелена на доступ
к данным



30% атак

направлены
на пользователей



4321

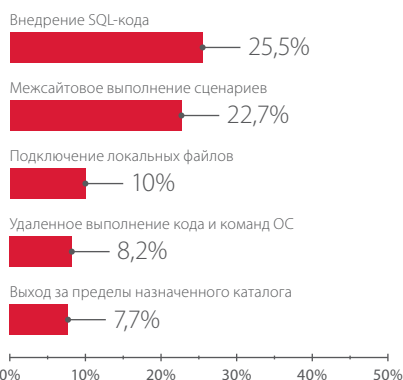
максимальное число атак
на одну компанию в сутки

Топ-5 источников атак по их количеству

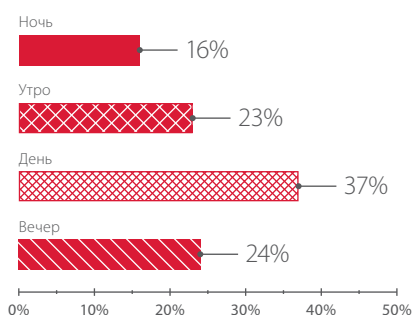
Россия — 46,6%
США — 14,5%
Франция — 6,6%
Германия — 3,7%
Нидерланды — 3,3%

Топ-5 источников атак по числу уникальных IP-адресов

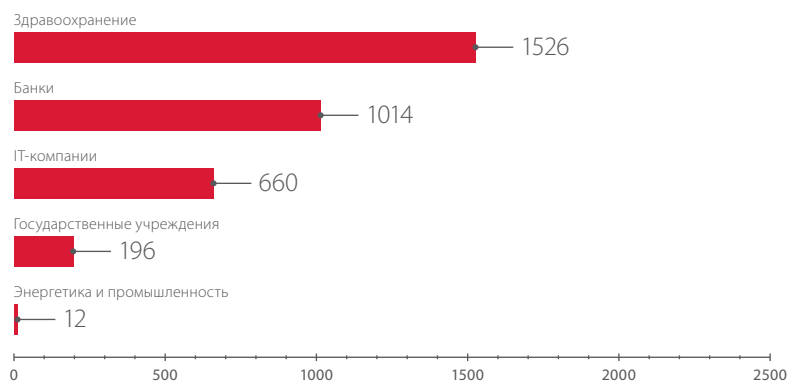
Россия — 58%
США — 8,7%
Китай — 3,8%
Украина — 3,6%
Франция — 2,6%



Самые распространенные атаки



Распределение атак по времени суток (по местному времени исследуемых организаций)



Среднее количество атак в день на одну компанию



СТАТИСТИКА АТАК НА ВЕБ-ПРИЛОЖЕНИЯ

Типы атак

В III квартале 2017 года самой распространенной была атака «Внедрение SQL-кода»; в случае ее успешной реализации злоумышленник может получить несанкционированный доступ к чувствительной информации или выполнить команды ОС. На втором месте рейтинга атака на пользователей веб-приложения «Межсайтовое выполнение сценариев». Как мы и прогнозировали в прошлом квартале, эти типы атак по-прежнему составляют практически половину от всех атак на исследуемые веб-приложения. Выросла доля атак «Подключение локальных файлов», направленных на выполнение произвольного кода на атакуемом сервере. Данный тип атак занимает третье место в рейтинге. Кроме того, по сравнению с прошлым кварталом в два раза увеличилось число атак высокой степени риска «Удаленное выполнение кода и команд ОС», с помощью которых злоумышленник может получить полный контроль над сервером с веб-приложением.

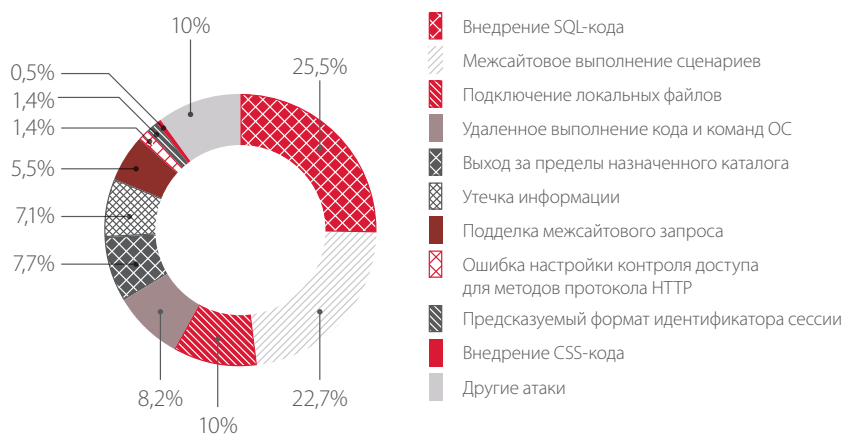


Рисунок 1. Типы атак на веб-приложения

Распределение атак по степени риска в соответствии с используемой в PT AF классификацией представлено на диаграмме ниже.

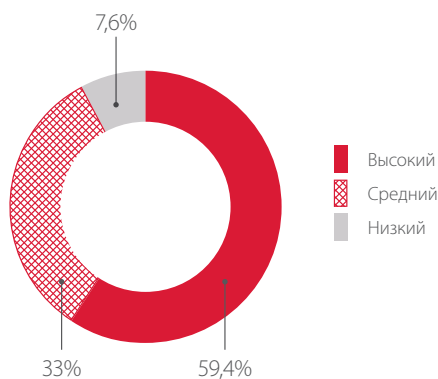


Рисунок 2. Распределение атак на веб-приложения по уровню риска

Полученные данные позволяют построить детальную статистику по атакам на веб-приложения для различных отраслей экономики. В III квартале в выборку попали веб-приложения учреждений сферы здравоохранения, энергетических и промышленных организаций, банков, IT-компаний и государственных учреждений.

Учреждения сферы здравоохранения

Статистика по самым распространенным атакам на веб-приложения сферы здравоохранения по сравнению с прошлым кварталом значительно отличается. Это отличие объясняется спецификой работы этих приложений. В основном исследованные в этом квартале веб-приложения используются в качестве информационных ресурсов и не используются для обработки персональных данных или сведений о состоянии здоровья пациентов. Именно отсутствием чувствительной информации, которая может представлять интерес для злоумышленников, объясняется значительное снижение доли атак «Внедрение SQL-кода» (с 46% до 2,9%) по сравнению с прошлым кварталом. При этом выросло число других атак, среди которых практически половина направлена на выполнение кода или команд ОС, в том числе при помощи подключения произвольных файлов. С помощью подобных атак злоумышленник может получить полный контроль над веб-приложением и затем подменять содержимое ресурса, нарушать его работу или распространять вредоносное ПО. Например, 24 октября этого года было зафиксировано начало распространения шифровальщика Bad Rabbit при помощи предварительно взломанных веб-ресурсов СМИ¹. При переходе на страницу взломанного веб-приложения пользователям предлагалось скачать фальшивый установщик Adobe Flash Player, запуск которого приводил к заражению их рабочих мест. Аналогичный сценарий с массовым распространением вредоносного ПО может быть реализован и для веб-ресурсов сферы здравоохранения, поскольку они, как и сайты СМИ и государственных учреждений, пользуются значительным спросом среди населения.

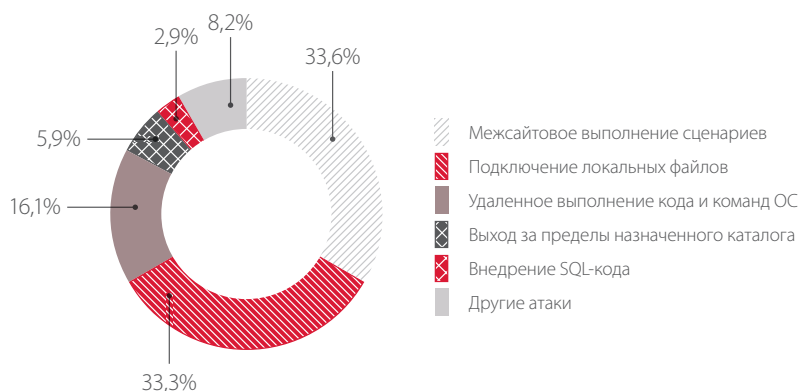


Рисунок 3. Типы атак на веб-приложения сферы здравоохранения

Промышленные и энергетические компании

Атаки на веб-приложения промышленных и энергетических компаний по-прежнему носят целенаправленный характер. Злоумышленники, атакуя подобные веб-приложения, пытаются получить чувствительную информацию о системе, которая может быть использована при планировании и проведении дальнейших атак. Как мы отмечали в исследованиях первого полугодия, злоумышленники пытаются использовать такие веб-приложения в качестве основной точки для проникновения во внутреннюю инфраструктуру компаний с последующим доступом к технологическим сегментам сети. Конечной целью подобных атак в основном является нарушение технологического процесса. Поэтому среди самых распространенных атак присутствуют те, которые позволяют удаленно выполнить команды ОС и захватить контроль над сервером и в дальнейшем развивать вектор атаки на внутреннюю инфраструктуру. По результатам наших исследований 77% всех выявленных в 2016 году векторов атак, позволивших преодолеть периметр корпоративной сети, были основаны именно на эксплуатации уязвимостей веб-приложений².

¹ welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

² Уязвимости корпоративных информационных систем (2017).

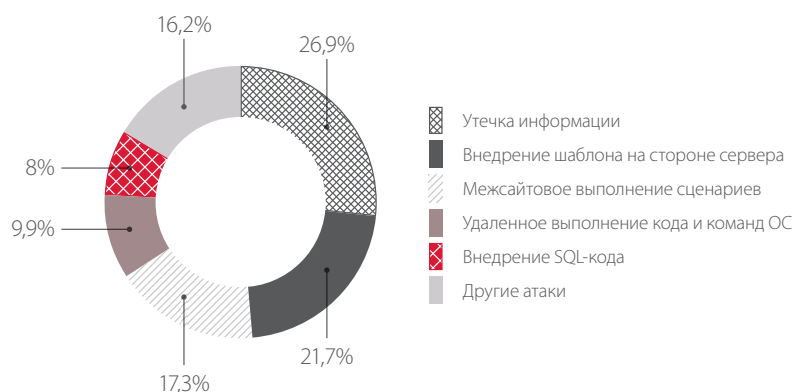


Рисунок 4. Типы атак на веб-приложения энергетических и промышленных компаний

Банки

Получение финансовой выгоды является основным мотивом злоумышленников при проведении атак на веб-ресурсы банков. С помощью атак «Внедрение SQL-кода» нарушители могут получить несанкционированный доступ к чувствительной информации, в том числе к персональным данным и финансовым сведениям клиентов банков. Кроме того, практически каждая третья атака направлена на пользователей веб-приложений. Злоумышленники пытаются выявить уязвимости, с помощью эксплуатации которых они смогут похищать учетные данные пользователей или заражать их рабочие станции вредоносным ПО. Успешная реализация таких атак может привести к финансовым потерям как для клиентов, так и для самого банка, а также негативно повлиять на его репутацию.

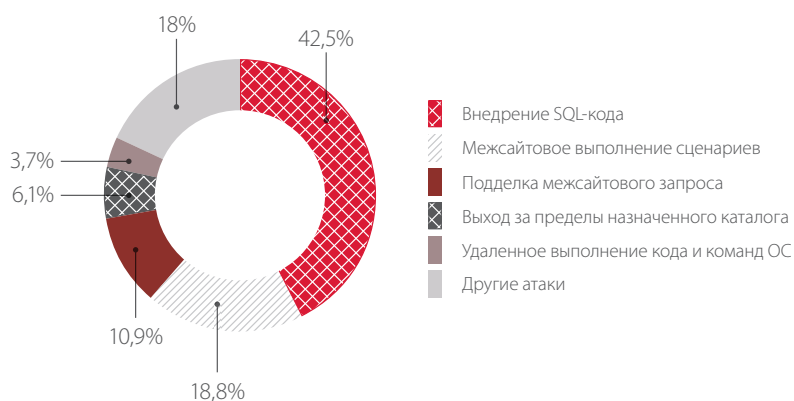


Рисунок 5. Типы атак на веб-приложения банков

IT-компании

Статистика по атакам на веб-приложения IT-компаний по сравнению с прошлым кварталом изменилась незначительно. Как и ранее, практически половину всех атак составляют «Внедрение SQL-кода» и «Межсайтовое выполнение сценариев». Данные атаки в первую очередь направлены на доступ к чувствительной информации и на получение учетных записей пользователей веб-приложений с целью последующего доступа к информационным ресурсам организации. Например, в случае успешной атаки «Межсайтовое выполнение сценариев» злоумышленник может получить cookie пользователя и осуществить доступ к portalу, который компания использует для взаимодействия с партнерами. Часто на таких ресурсах обрабатывается чувствительная информация, которая представляет высокую ценность для злоумышленников. Кроме того, особый интерес для злоумышленников представляют учетные данные привилегированных пользователей, которые обладают административными правами и часто используют одну и ту же учетную запись для доступа к нескольким веб-приложениям и portalам. Поэтому атаки «Внедрение SQL-кода» и «Межсайтовое выполнение сценариев» могут быть направлены именно на получение учетных данных администраторов веб-приложений. В итоге доступ нарушителя к партнерским portalам и другим веб-приложениям может принести IT-компаниям существенные репутационные и, возможно, финансовые потери.

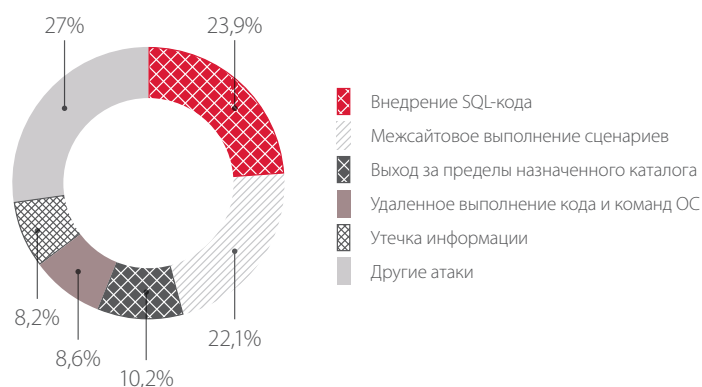


Рисунок 6. Типы атак на веб-приложения IT-компаний

Государственные учреждения

Большая часть веб-приложений государственных учреждений, рассматриваемых в рамках данного исследования, используется для обработки персональных данных граждан России или применяется в качестве информационных и новостных ресурсов. Каждая пятая атака злоумышленников направлена на несанкционированный доступ к чувствительной информации, каждая вторая — на пользователей веб-приложения. Злоумышленники пользуются тем, что большинство пользователей таких веб-ресурсов очень плохо осведомлены в вопросах информационной безопасности. Основная цель нарушителей — получение персональных данных пользователей.

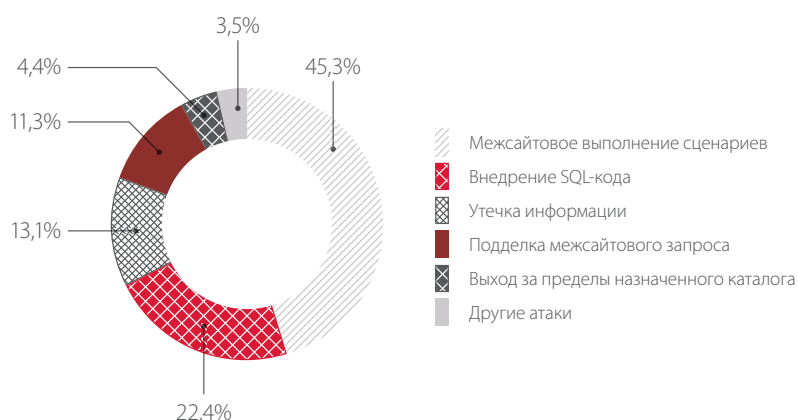


Рисунок 7. Типы атак на веб-приложения госучреждений

Среднее количество атак по отраслям

По среднему числу зарегистрированных событий в день в этом квартале на первом месте находятся учреждения сферы здравоохранения. Такое увеличение количества атак по сравнению с прошлым кварталом объясняется тем, что данные веб-ресурсы являются основными новостными источниками в сфере здравоохранения для крупных регионов России.

Значительное снижение числа атак на веб-приложения государственных учреждений связано с тем, что в выборку в этот раз попали веб-приложения местного, районного значения, которые посещают меньшее количество пользователей, чем веб-ресурсы, исследованные в прошлом квартале. В целом различие в количестве атак на веб-ресурсы регионального и районного масштабов объясняется тем, что злоумышленники в ходе своих атак стремятся получить большую выгоду и охватить максимальное количество жертв. Поскольку веб-ресурсы регионального значения посещает большее количество пользователей и часто на таких веб-ресурсах обрабатывается больший объем чувствительной информации, успешные атаки на такие приложения приведут к более значимым последствиям, чем аналогичные атаки на веб-ресурсы местного уровня.

Как и в прошлом квартале, среднее количество атак на компании промышленного сектора не превышает двух десятков, что подтверждает наше предположение о целевом характере атак на такие веб-ресурсы. Злоумышленники стараются действовать максимально скрытно, их основная цель — получить доступ к ресурсам внутренней сети с последующим развитием атаки на технологический сегмент. В результате именно такие единичные атаки могут привести к чрезвычайно опасным последствиям — от нарушения или остановки технологического процесса до опасных техногенных последствий, экологических катастроф и человеческих жертв.

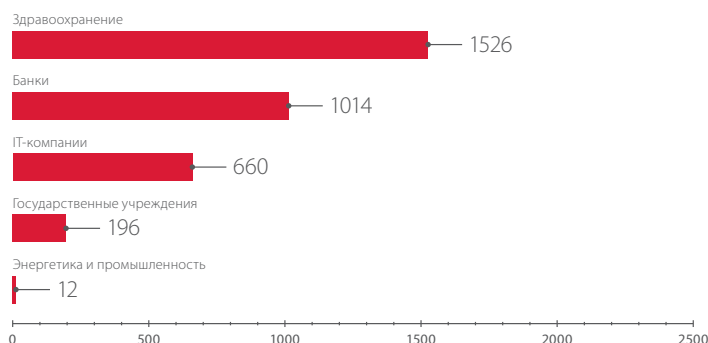


Рисунок 8. Среднее число атак в день по отраслям

Примеры атак

При анализе результатов пилотного проекта для учреждения сферы здравоохранения в течение нескольких дней фиксировались множественные атаки «Подключение локальных файлов». Например, 9 июля во второй половине дня злоумышленники с нескольких десятков IP-адресов пытались провести атаки, направленные на выполнение произвольного кода на атакуемом сервере. В итоге тип атак «Подключение локальных файлов» вышел на второе место в рейтинге самых распространенных атак для веб-приложений сферы здравоохранения и на третье место в общем рейтинге по всем пилотным проектам.

ATTACKS					
0 to 40 of 260 available for paging					
EVENT_SEVERITY	EVENT_TAG.NAME	EVENT_DESCRIPTOR	POLICY_NAME	MATCHED_VARIABLES	TIMESTAMP
high	Local File Inclusion	A Local File Inclusion...	Default	REQUEST_ARGS....	2017-07-09 22:33:28
high	Local File Inclusion	A Local File Inclusion...	Default	REQUEST_ARGS....	2017-07-09 22:33:26
high	Local File Inclusion	A Local File Inclusion...	Default	REQUEST_ARGS....	2017-07-09 22:32:59
high	Local File Inclusion	A Local File Inclusion...	Default	REQUEST_ARGS....	2017-07-09 22:32:59
high	Local File Inclusion	A Local File Inclusion...	Default	REQUEST_ARGS....	2017-07-09 22:32:58

Рисунок 9. Атаки «Подключение локальных файлов» 9 июля (интерфейс PT AF)

```

Raw request
1 GET /scripts/index.php?pathPrefix=../../../../../../../../../../../../../../../../boot.ini HTTP/1.1
2 Connection: Keep-Alive
3 Host:
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent:
7 Accept: image/gif, image/x-bitmap, image/jpeg, image/png, image/pjpeg, image/png, */*
8 Accept-Language: en
9 Accept-Charset: iso-8859-1,*utf-8
10
11

```

Рисунок 10. Пример запроса в рамках атаки «Подключение локальных файлов» (интерфейс PT AF)

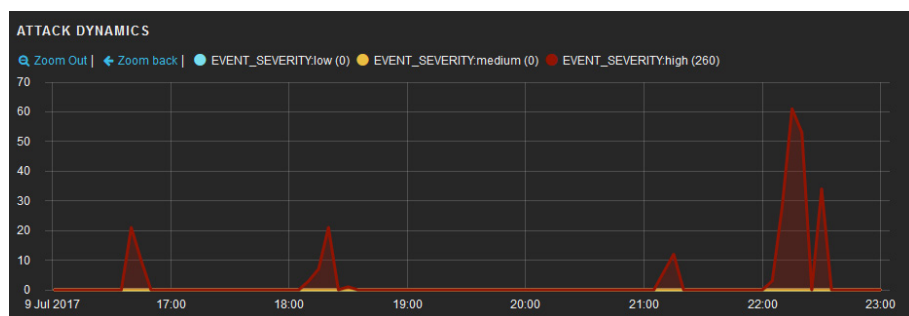


Рисунок 11. Динамика атак «Подключение локальных файлов» 9 июля (интерфейс PT AF)

В ходе другого пилотного проекта была обнаружена цепочка атак, направленных на получение информации при помощи эксплуатации уязвимости [CVE-2017-9798](#) в веб-сервере Apache. Данная уязвимость и атака, направленная на ее эксплуатацию, называются Optionsbleed. Злоумышленник, используя HTTP-метод OPTIONS, может получить доступ к фрагментам памяти, содержащим остаточные данные от обработки текущим процессом запросов остальных клиентов системы совместного хостинга. Подробная информация о деталях эксплуатации уязвимости была опубликована 18 сентября этого года, а первые попытки ее эксплуатации были зафиксированы нами уже через 3 часа и на следующий день их стало еще больше. Такой короткий промежуток времени между публикацией уязвимости и началом практического применения объясняется низкой сложностью ее эксплуатации. Кроме того, для эксплуатации данной уязвимости практически сразу был подготовлен и опубликован общедоступный эксплойт³.

```
Raw request
1 OPTIONS / HTTP/1.1
2 Host:
3 X-Orator-IP-Source:
4 X-Orator-TCP-Info: 51927, 70000, 35000
5 X-Forwarded-For:
6 Content-Length: 0
7 Accept-Encoding: gzip, deflate
8 Accept: */*
9 User-Agent:
10
11
```

Рисунок 12. Пример запроса в рамках атаки Optionsbleed (интерфейс PT AF)

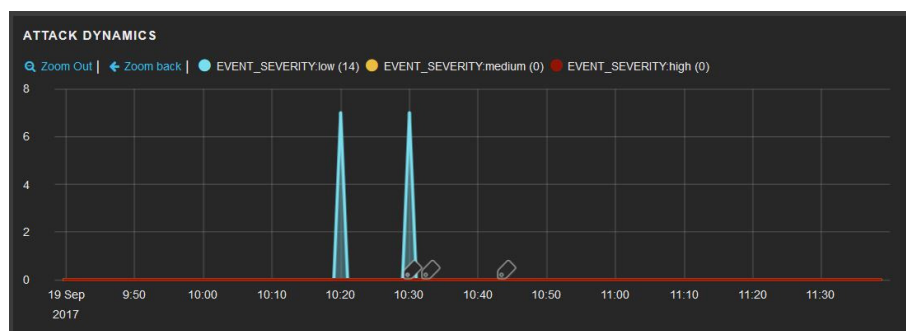


Рисунок 13. Динамика атак Optionsbleed 19 сентября (интерфейс PT AF)

19 сентября в течение десятиминутного промежутка времени были зафиксированы атаки Optionsbleed, которые межсетевой экран в режиме реального времени объединил в две корреляционные цепочки.

ALERTS			
ALERT_SEVERITY	STATUS	ALERT_NAME	TIMESTAMP
	finished	OPTIONSBLEED Attack	2017-09-19 10:30:32
View: Basic / Advanced / Raw			
Field	Value		
Description	Alert name: OPTIONSBLEED Attack (https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-leak-Apaches-server-memory.html)		
Severity summary	High: 0 Medium: 0 Low: 7		
Date	Start: 2017-09-19 10:30:32 End: 2017-09-19 10:32:38		
Correlation	59c0c94605367c18e174a1e5 Default:37.48.115.230.1505806232		
Policy	Default		
Status	FINISHED		

Рисунок 14. Пример одной из выявленных цепочек атак Optionsbleed (интерфейс PT AF)

Атакам Optionsbleed присвоен низкий уровень риска, так как в случае успешной атаки злоумышленник может получить лишь несколько байтов памяти, что не приведет к раскрытию большого объема чувствительной информации. Кроме того, проблема актуальна только для систем совместного хостинга, на которых размещаются сайты разных пользователей, и только в том случае, если в файле .htaccess установлена директива Limit для HTTP-метода,

³ rapid7.com/db/modules/auxiliary/scanner/http/apache_optionsbleed

ATTACKS					
EVENT_TAG.NAME ▶	◀ EVENT_SEVERITY ▼	◀ EVENT_DESCRIPTION...	◀ POLICY_NAME ▶	◀ MATCHED.VARIABLE...	◀ TIMESTAMP ▶
OPTIONSBLEED	low		Default	REQUEST_METHOD	2017-09-19 10:30:28
OPTIONSBLEED	low		Default	REQUEST_METHOD	2017-09-19 10:30:29
OPTIONSBLEED	low		Default	REQUEST_METHOD	2017-09-19 10:30:30
OPTIONSBLEED	low		Default	REQUEST_METHOD	2017-09-19 10:30:33
OPTIONSBLEED	low		Default	REQUEST_METHOD	2017-09-19 10:30:35
OPTIONSBLEED	low		Default	REQUEST_METHOD	2017-09-19 10:30:36
OPTIONSBLEED	low		Default	REQUEST_METHOD	2017-09-19 10:30:37

Рисунок 15. Атаки Optionsbleed, входящие в одну корреляционную цепочку (интерфейс PT AF)

не зарегистрированного глобально на сервере. Для защиты от атак данного типа необходимо установить актуальную версию веб-сервера Apache.

Как и в прошлом квартале, были обнаружены попытки удаленного выполнения команд при помощи эксплуатации недавно опубликованной уязвимости [CVE-2017-5638](#) во фреймворке Apache Struts.

```
Raw request
1 GET / HTTP/1.1
2 Host:
3 Connection: keep-alive
4 User-Agent:
5 Content-Type: {({nike="multipart/form-data").(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#mem
berAccess={#memberAccess=#dm}) * ((#container=#context['com.opensymphony.xwork2.ActionContext.container']
ber')).(#ognlUtil=#container.getInstance((com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil
.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAd
cess(#dm))).(#cmd='echo CVE-2017-5638 check').(#iswin=@java.lang.System@getProperty('os.name')).
toLowerCase().contains('win')).(#cmds=(#iswin?('#cmd.exe', '/c', #cmd):('/bin/bash', '-c', #cmd))).(#
new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=@
org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(#os=@org.apache.commons.io
.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

Рисунок 16. Запрос, направленный на эксплуатацию уязвимости CVE-2017-5638 (интерфейс PT AF)

Важно отметить, что злоумышленники активно следят за публикацией информации о новых уязвимостях и при планировании и проведении атак учитывают, что на целевой системе могут не быть установлены последние обновления. Поэтому часть атак всегда будет направлена на эксплуатацию недавно обнаруженных уязвимостей, что подтверждается примером с атакой Optionsbleed. Именно поэтому так важно стремиться быть на шаг впереди злоумышленников и своевременно устанавливать обновления для всех компонентов веб-приложения.

Источники атак

По итогам анализа статистики количества атак для всех исследуемых веб-приложений было установлено, что практически половина атак производится с российских IP-адресов. Кроме того, по числу атак с уникальных IP-адресов со значительным отрывом также лидирует Россия. Это объясняется тем, что основная часть пилотных проектов по внедрению РТ АФ проводилась для российских компаний. По сравнению с итогами прошлых кварталов распределение атак по их источникам изменилось незначительно. Как и прежде, — помимо России — США, Франция, Германия, Нидерланды, Китай и Украина занимают верхние строки рейтинга как по количеству атак, так и по числу уникальных IP-адресов, с которых производились эти атаки.

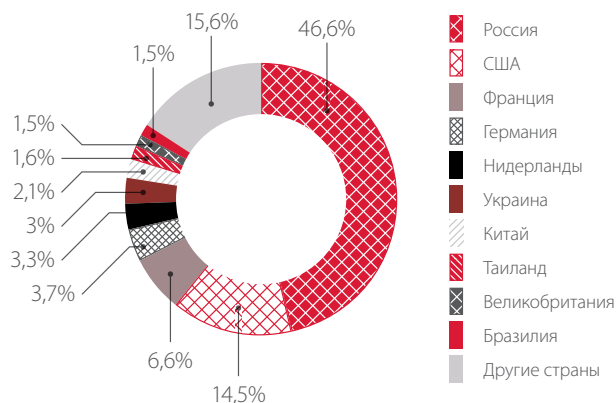


Рисунок 17. Доли атак по их источнику

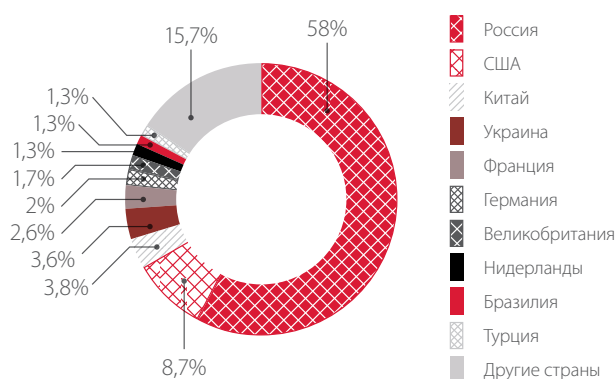


Рисунок 18. Уникальные IP-адреса, с которых производятся атаки

Динамика атак

По результатам анализа статистической информации за III квартал года можно оценить распределение атак по времени. Для этого рассмотрим динамику атак в зависимости от их типа для веб-приложений одной из исследуемых в этом квартале компаний. За основу для построения диаграммы были взяты 10 наиболее распространенных типов атак. Затем для каждого типа атак было посчитано их количество в сутки. На диаграмме учтены данные за весь квартал. Полученное распределение позволяет оценить, какие атаки выделяются из общего потока по количеству отправленных нарушителями запросов.

По среднему количеству атак со значительным отрывом выделяются «Внедрение SQL-кода» и «Межсайтовое выполнение сценариев» — самые распространенные типы атак как в этом квартале, так и в предыдущие периоды исследования. В отдельные дни зафиксированы множественные атаки «Межсайтовое выполнение сценариев», количество которых в разы превышает среднее значение за весь квартал. При этом отмечены длительные периоды, в которые значительно снижалась интенсивность атак данного типа и их количество составляло меньше двух десятков в сутки.

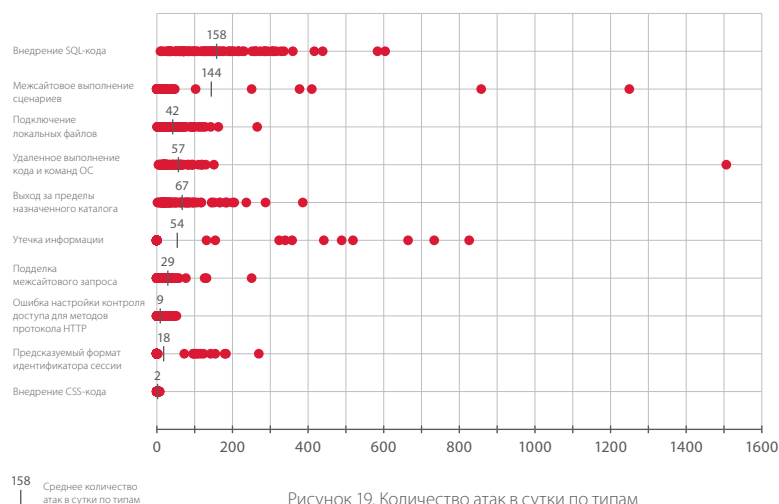


Рисунок 19. Количество атак в сутки по типам

Количество атак «Внедрение SQL-кода» и «Подключение локальных файлов» оставалось стабильным на протяжении всего квартала и редко превышало порог в 400 и 200 атак в сутки соответственно. Подобная динамика объясняется тем, что для успешной реализации перечисленных атак нарушителю необходимо подобрать некорректно фильтруемые символы либо имена сценариев, каталогов и файлов, поэтому одна атака разбивается на множество попыток, которые детектируются РТ АФ в виде цепочки.

Отдельно можно отметить день, в который наблюдалось значительное увеличение количества атак «Удаленное выполнение кода и команд ОС». Такое превышение среднего количества злонамеренных запросов связано с аномальной активностью злоумышленников, которые в течение суток пытались получить контроль над веб-ресурсами исследуемой компании.

Среднее количество атак других типов не превышает 70 в сутки.

Аналогичным образом можно рассмотреть распределение суточного количества атак по дням недели.

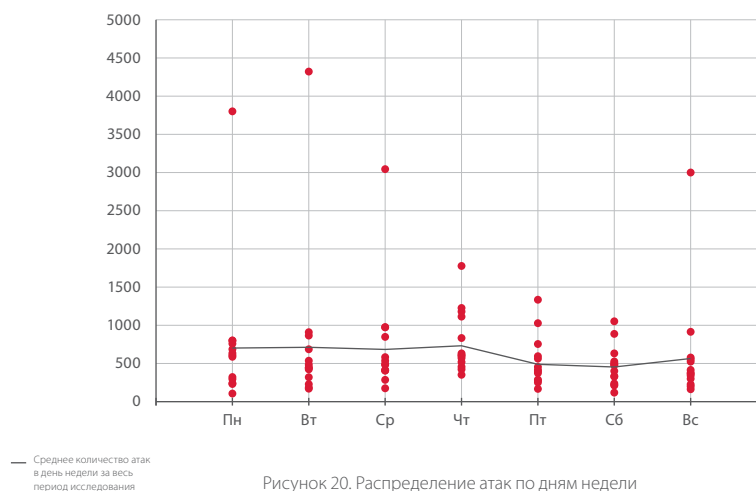


Рисунок 20. Распределение атак по дням недели

В среднем число атак в сутки варьировалось от 500 до 700 и крайне редко опускалось ниже 200. Кроме того, важно отметить, что злоумышленники пытаются использовать любую возможность для получения выгоды и проводят атаки не только в рабочие дни организаций, но и в выходные. Максимальное количество зафиксированных атак в день составило 4321.

Из трех месяцев, в течение которых проводилось исследование, было выделено 4 дня, когда суммарное значение атак превышало 3000.

Динамику атак можно оценить не только по дням недели, но и по времени суток. При построении диаграммы учитывалось местное время организации.

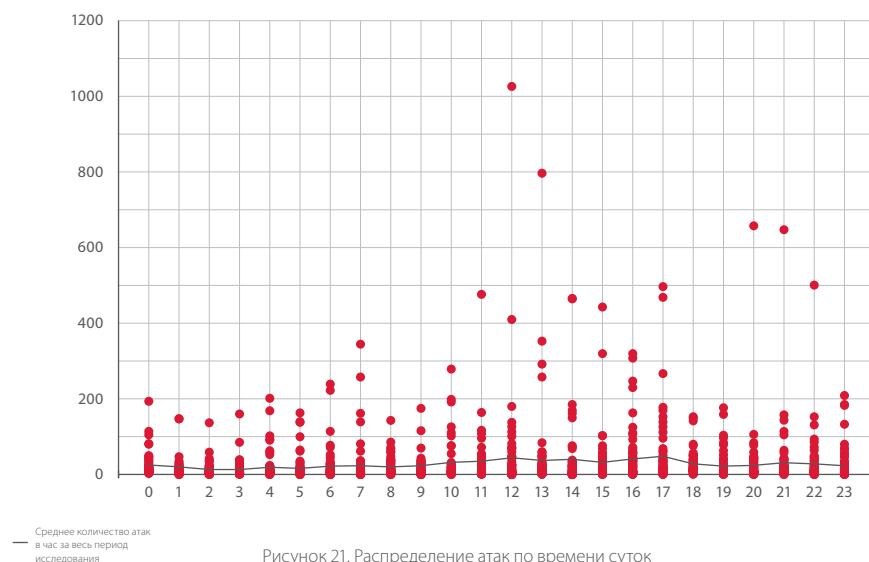


Рисунок 21. Распределение атак по времени суток

Можно отметить увеличение интенсивности атак в дневные и вечерние часы. При этом отдельные пиковые значения числа атак могут быть зафиксированы в любое время суток. В качестве примера рассмотрим график атак за 15 августа. В этот день пиковые значения зафиксированы как в первую, так и во вторую половину дня.

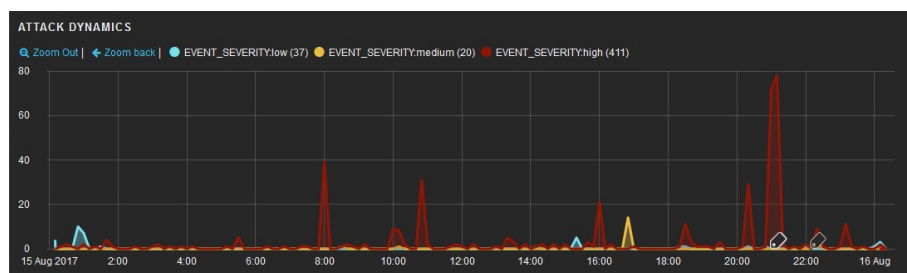


Рисунок 22. Динамика атак на ресурсы исследуемой компании 15 августа (интерфейс PT AF)

Такие результаты объясняются двумя основными факторами. Увеличение числа атак в дневные и вечерние часы связано с активностью пользователей веб-ресурсов: именно на них направлена большая часть атак в этот период времени. Что касается атак в ночные и утренние часы, то злоумышленники проводят их с расчетом, что служба безопасности компании не сможет своевременно обнаружить атаку и отреагировать должным образом. В качестве меры защиты, направленной на круглосуточное обнаружение и предотвращение атак злоумышленников, можно использовать межсетевой экран уровня приложений.

Типы используемых атак и их распределение по дням и часам могут отличаться в зависимости от функциональности веб-приложения и специфики работы атакуемой компании. Кроме того, важно помнить, что абсолютно любое веб-приложение может оказаться под ударом в случае массовых атак, например направленных на тестирование и отладку новых эксплойтов на случайных сайтах или целом списке IP-адресов. Такие риски стоит учитывать при организации системы защиты веб-приложения.

ВЫВОДЫ

В III квартале 2017 года веб-приложения вне зависимости от функциональных особенностей по-прежнему остаются привлекательной мишенью для злоумышленников. Большая часть зафиксированных атак, как и в прошлые периоды, направлена на доступ к чувствительной информации и на пользователей веб-приложений.

Злоумышленники готовы к атакам 24 часа в сутки без выходных и праздников. Они активно собирают сведения о новых уязвимостях, разрабатывают и тестируют эксплойты. При этом далеко не все компании успевают своевременно обновлять компоненты своих веб-приложений, установить необходимые патчи. И в итоге злоумышленники успешно эксплуатируют новые уязвимости. Чтобы минимизировать последствия от таких атак, необходимо не только вовремя обновлять программное обеспечение, но и использовать превентивные средства защиты, такие как межсетевой экран уровня приложений, для обнаружения и предотвращения атак на веб-ресурсы.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.