АТАКИ НА ВЕБ-ПРИЛОЖЕНИЯ

2016

POSITIVE TECHNOLOGIES

Содержание

Введение

Общедоступные веб-приложения являются привлекательной мишенью для злоумышленников. Атаки на веб-приложения открывают перед ними широкие возможности: доступ к внутренним ресурсам компании, чувствительной информации, нарушение функционирования приложения или обход бизнес-логики — практически любая атака может принести финансовую выгоду для злоумышленника и убытки, как финансовые, так и репутационные — для владельца веб-приложения. Кроме того, под угрозой находятся и пользователи веб-приложений, поскольку успешные атаки позволяют похищать учетные данные, выполнять действия на сайтах от лица пользователей, а также заражать рабочие станции вредоносным ПО.

При исследовании атак на веб-приложения мы, в первую очередь, ставили перед собой задачу установить, какие атаки пользуются наибольшей популярностью у злоумышленников и каковы возможные мотивы их действий, а также определить основные источники угроз для различных отраслей. Такие данные позволяют понять, каким аспектам следует уделить внимание при обеспечении безопасности веб-приложений. Кроме того, мы рассмотрим распределение типов атак и активности злоумышленников в зависимости от сферы деятельности компании, а также динамику изменения характера атак в течение года.

Для сбора исходных данных по атакам мы использовали данные, полученные в ходе пилотных проектов по внедрению PT Application Firewall (PT AF) в 2016 году. Межсетевые экраны прикладного уровня (web application firewalls, WAF) являются необходимым элементом защиты веб-приложений от атак злоумышленников. В отличие от обычных межсетевых экранов и систем предотвращения вторжений WAF должен не только обнаруживать и предотвращать известные атаки на уровне приложения и бизнес-логики, но и выявлять эксплуатацию уязвимостей нулевого дня, предотвращать атаки на пользователей, анализировать и сопоставлять множество событий для выявления цепочек атак, что возможно только при использовании инновационных технологий нормализации, эвристического и поведенческого анализа и самообучения.

В пилотных проектах принимали участие государственные учреждения, организации сферы образования, финансов, транспорта, промышленности и IT. Среди рассматриваемых систем присутствуют как российские компании, так и зарубежные. В первой части исследования отражены результаты, полученные на основе данных, собранных в ходе этих проектов.

Поскольку PT AF используется и для защиты ресурсов Positive Technologies, вторая часть исследования основана на данных о выявленных атаках на веб-приложения компании, которые мы собирали в течение 2016 года.

Все приведенные в данном исследовании примеры атак были проверены вручную на предмет ложных срабатываний и являются достоверными.

Результаты пилотных проектов по внедрению PT Application Firewall

Наиболее часто в ходе пилотных проектов встречались «Внедрение операторов SQL» и «Выполнение команд ОС», такие атаки PT AF фиксировал более чем в 80% систем. Path Traversal занимает второе место по популярности среди выявленных атак. Очевидно, что в первую очередь злоумышленники пробуют применить наиболее простые атаки, не требующие особых условий для выполнения. В основном более низкий процент обнаружения атаки свидетельствует о более высоком уровне сложности или необходимости специальных условий для ее реализации, например, наличия функции загрузки файлов в веб-приложении или совершения определенных действий со стороны пользователей.

При составлении рейтинга наиболее популярных атак мы исключили атаки, которые осуществлялись специальным ПО для автоматизированного сканирования веб-приложения на наличие уязвимостей, например, Acunetix, sqlmap.

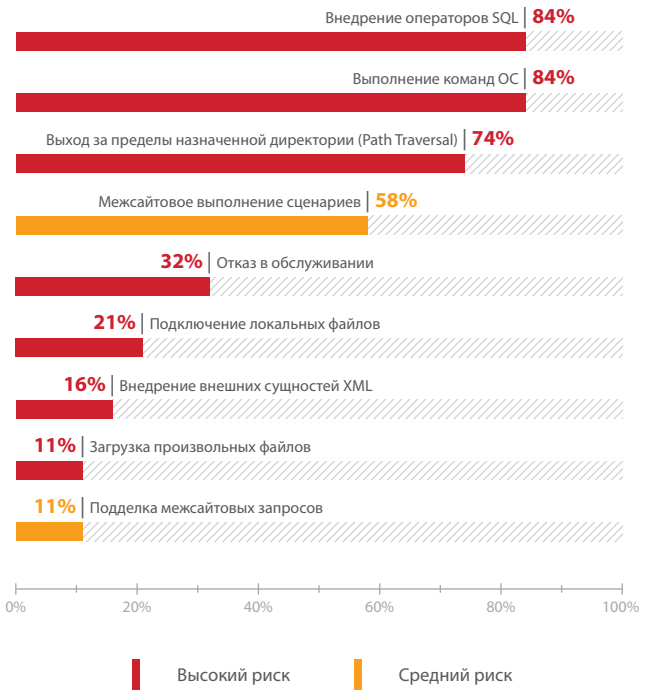

Рис. 1. Рейтинг наиболее популярных атак (доли веб-приложений)

Большинство атак в этом рейтинге эксплуатируют критически опасные уязвимости и могут привести к полной компрометации веб-приложения и сервера, что может позволить злоумышленнику получить доступ к ресурсам локальной сети.

Соотношение типов атак, зафиксированных в ходе работы PT AF, и их количество меняются в зависимости от отрасли, к которой относится исследуемая система. Злоумышленники преследуют разные цели, при этом уровень квалификации и технические возможности нарушителей также различаются. На приведенных диаграммах представлены среднее количество атак в день на одну систему, а также соотношение количества атак, выполняемых вручную и с использованием утилит для автоматизированного сканирования.

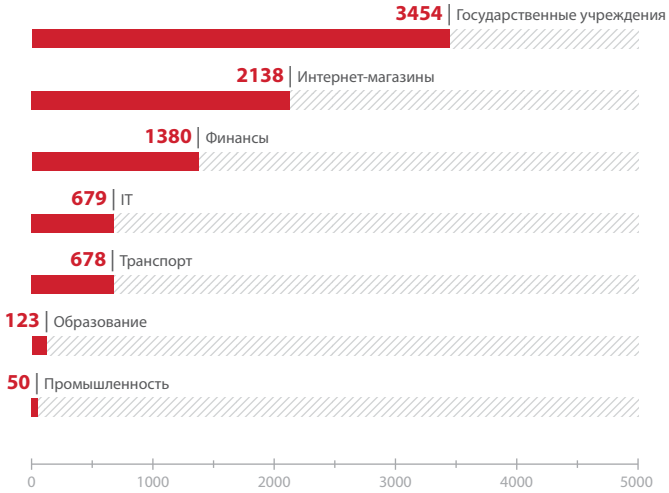

Рис. 2. Среднее количество атак в день на одну систему

Рис. 3. Соотношение автоматизированного сканирования и атак, выполняемых вручную

Большую часть атак для всех отраслей, кроме государственных учреждений и интернет-магазинов, составляют атаки, выполняемые при помощи специализированного ПО для поиска уязвимостей. Автоматизированное сканирование включает в себя попытки выполнения различных видов атак, например, внедрения операторов SQL, Path Traversal, с использованием готовых программных средств инструментального анализа защищенности. Результаты сканирования могут быть использованы злоумышленником для эксплуатации уязвимостей и дальнейшего развития вектора атаки до получения доступа к чувствительной информации, ресурсам локальной сети, критически важным системам или для проведения атак на пользователей.

На рисунке ниже приведен пример обнаружения автоматизированного сканирования с помощью утилиты sqlmap. PT AF выявил нежелательное содержание HTTP-заголовка User-Agent и запрос, содержащий внедрение операторов SQL.

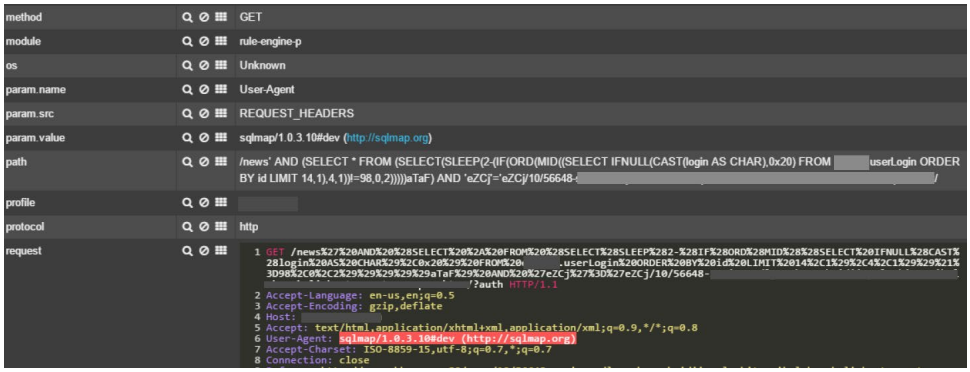

Рис. 4. Пример обнаружения автоматизированного сканирования

Наибольшее среднее количество атак в день — приблизительно 3500 атак — зафиксировано в ходе пилотных проектов в государственных учреждениях. Автоматизированный поиск уязвимостей составляет всего 18% от общего числа атак. Интернет-магазины занимают вторую строчку в этом рейтинге: в день регистрировалось около 2200 атак, при этом практически все они проводились без использования автоматизированных средств сканирования.

В финансовой сфере PT AF регистрировал около 1400 атак в день, среди которых преобладал автоматизированный поиск уязвимостей. На транспортные ресурсы и IT-компании приходится в среднем около 680 атак в день, большую часть которых также составляет автоматизированный поиск уязвимостей.

Из расчетов среднего количества атак в день для сферы образования был исключен информационно-аналитический центр, в функции которого входит обработка результатов государственных экзаменов. Пилотный проект для этого центра проходил в летнее время, когда учащиеся школ сдавали ЕГЭ и ГИА, в связи с чем наблюдалось чрезвычайно большое число атак на веб-приложение — более 20 000 атак в день. При этом самыми распространенными являлись атаки с использованием инструментальных средств сканирования на наличие уязвимостей. Учащиеся, обладая базовыми знаниями об информационной безопасности и способах обхода механизмов защиты, могли использовать общедоступное ПО для сканирования системы. Этим объясняется и тот факт, что большая часть атак данного типа исходила со стороны США: вероятно, публичные утилиты или онлайн-сервисы использовали прокси-серверы, расположенные на территории США. Целью атак на информационно-аналитический центр, скорее всего, был доступ к результатам экзаменов и экзаменационным материалам. Возможно, учащиеся считали, что таким образом смогут изменить свои баллы, полученные за экзамен. Кроме того, можно предположить, что злоумышленники пытались найти уязвимости, эксплуатация которых позволила бы получить доступ к базам экзаменационных материалов для последующего нелегального распространения.

Для промышленных систем PT AF зафиксировал около 50 атак в день, практически все представляли собой автоматизированный поиск уязвимостей, и лишь 2% проводились вручную.

На следующей диаграмме для каждой отрасли представлено соотношение типов атак, осуществляемых злоумышленниками, при этом из расчетов были исключены атаки, совершаемые в рамках автоматизированного сканирования на наличие уязвимостей, поскольку они не являются специфичными для конкретных отраслей.

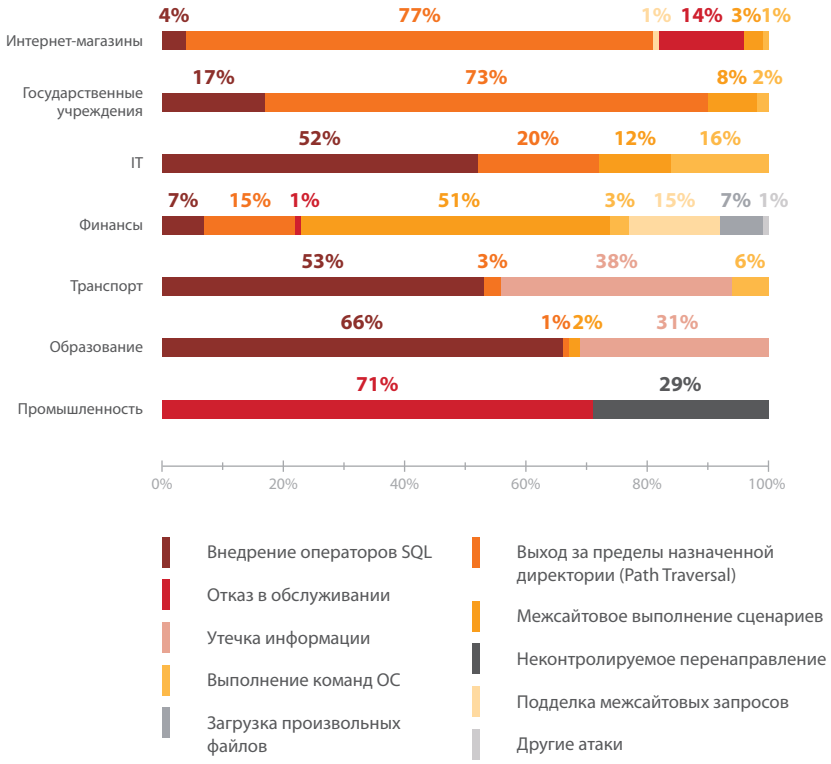

Рис. 5. Соотношение типов атак, выполняемых вручную

Для государственных учреждений более 70% составили атаки Path Traversal, с помощью которых злоумышленники пытались выйти за пределы текущего каталога файловой системы и получить доступ к файлам, находящимся на сервере, с целью хищения чувствительной информации.

Пример обнаружения атаки Path Traversal представлен ниже. Злоумышленник намеревался выйти в корневую директорию сервера и получить доступ к файлу /etc/passwd, который содержит список учетных записей пользователей системы.

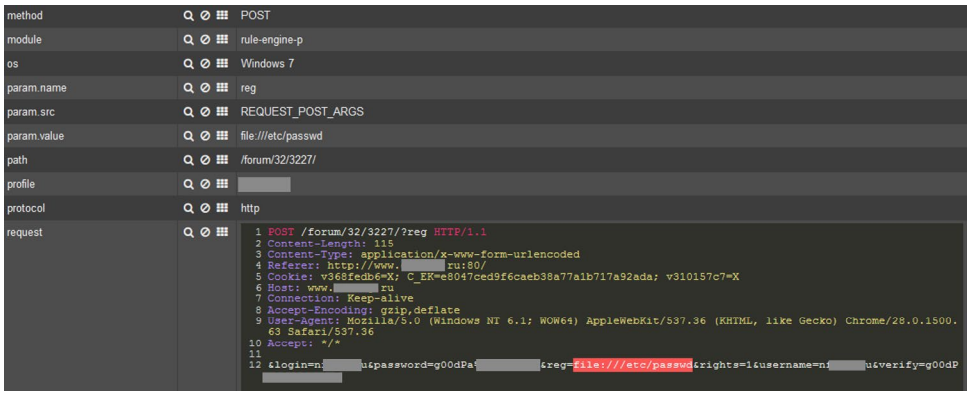

Рис. 6. Пример обнаружения атаки «Path Traversal»

Около 17% атак являются попытками внедрения операторов SQL. Небольшую часть (около 8%) составляют атаки «Межсайтовое выполнение сценариев», направленные на пользователей порталов государственных услуг. Выполнить команды ОС злоумышленники пытались в 2% случаев.

Почти три четверти атак на интернет-магазины составили атаки Path Traversal. Так же, как и на порталах, предоставляющих государственные услуги, злоумышленники предпринимали попытки выйти за пределы текущего каталога файловой системы. Существенную часть (14%) составляют атаки на отказ в обслуживании. Для интернет-магазина угроза нарушения доступности веб-приложения является критической. Атаки на пользователей («Межсайтовое выполнение сценариев» и «Подделка межсайтовых запросов») в сумме составляют 4%. В 4% случаев встречается и внедрение операторов SQL.

В финансовой сфере около 65% в совокупности составили атаки «Межсайтовое выполнение сценариев» и «Подделка межсайтовых запросов», направленные на пользователей систем. Такие атаки широко распространены в финансовой отрасли и представляют особую опасность, поскольку позволяют похищать значения Cookie и учетные данные пользователей (при помощи фишинга), а также совершать действия от лица легитимных пользователей.

На рисунке приведен пример выявления атаки «Межсайтовое выполнение сценариев». Злоумышленник пытался вывести на экран значения Cookie для проверки уязвимости веб-приложения к этой атаке.

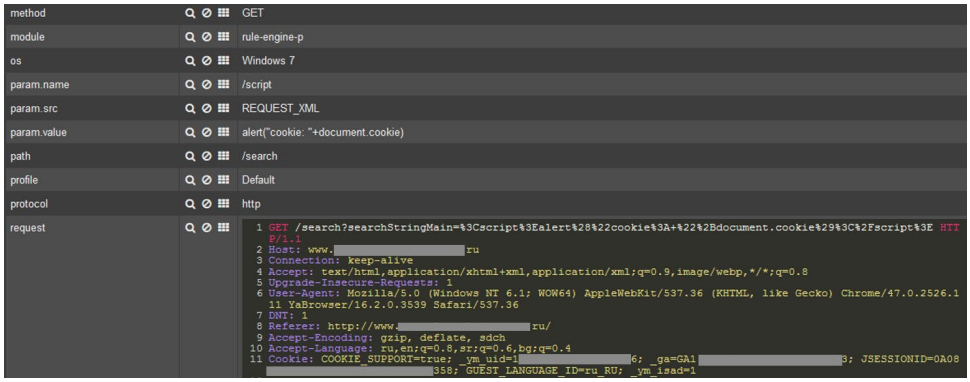

Рис. 7. Пример обнаружения атаки «Межсайтовое выполнение сценариев»

Злоумышленники пробовали получить доступ к чувствительной информации с помощью атаки Path Traversal (15% от общего числа) и внедрения операторов SQL (7% от общего числа). Доля атак «Загрузка произвольных файлов» составила 7%. Подобные атаки часто используются для получения доступа к выполнению команд ОС, при этом непосредственное выполнение команд ОС было зарегистрировано в 3% случаев. В целом, характер и сложность атак свидетельствуют о более высоком уровне технической подготовки злоумышленников по сравнению с другими рассматриваемыми отраслями.

В сфере IT более половины зафиксированных атак являются попытками внедрения операторов SQL. Присутствуют также атаки Path Traversal (20% от общего числа). Кроме того, 20% являются попытками выполнения команд ОС, а 12% атак на веб-приложения IT-компаний нацелены на пользователей систем.

Для веб-приложений транспортных компаний количество атак «Внедрение операторов SQL» превышает 50%, около 38% составляет утечка информации, и 6% — выполнение команд ОС.

В сфере образования приблизительно 70% атак, выполняемых вручную, составило «Внедрение операторов SQL». Эта атака зачастую является достаточно простой в исполнении, ее можно использовать для получения доступа к личным кабинетам пользователей или содержимому баз данных. Около 30% атак представляют собой эксплуатацию

уязвимости «Утечка информации», которая может позволить злоумышленнику получить чувствительные данные или узнать дополнительную информацию о системе.

На рисунке можно увидеть пример обнаружения внедрения операторов SQL, злоумышленник ввел свой запрос к базе данных в GET-параметре id для проверки возможности эксплуатации уязвимости.

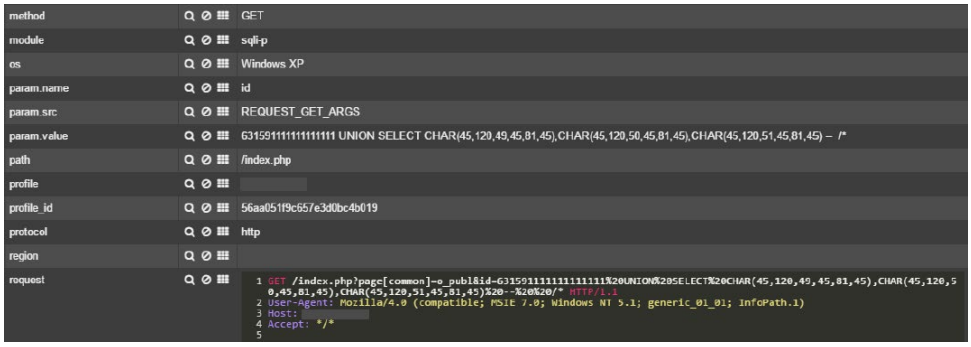

Рис. 8. Пример обнаружения атаки «Внедрение операторов SQL»

Почти две трети атак на приложения промышленных предприятий составили атаки на отказ в обслуживании, а остальные представляли собой неконтролируемое перенаправление.

Анализ источников атак проводился только в отношении российских систем, участвовавших в пилотных проектах. Наибольшее число зафиксированных атак исходят из русскоговорящих стран, на первых позициях находятся Россия и Украина. Достаточно высок процент атак, источником которых являются Нидерланды и США, поскольку на территории этих стран находится большое число провайдеров, предоставляющих услуги прокси-серверов.

Источники внешних атак на российские организации различаются в зависимости от отрасли.

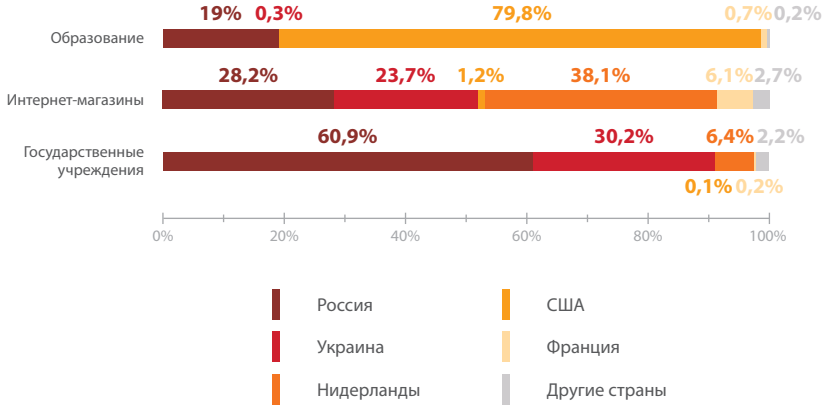

Рис. 9. Внешние источники атак по отраслям

Большая часть атак на государственные учреждения совершается с российских IP-адресов, около трети совершаются с IP-адресов, принадлежащих украинским провайдерам, в 6% случаев источником являются Нидерланды.

Источником атак для интернет-магазинов приблизительно в равных долях (около четверти от общего числа) являются Россия и Украина. Более трети атак проходит через IP-адреса Нидерландов.

Для атак на сферу образования, как было показано выше, широко используются публичные сервисы и утилиты для сканирования веб-приложений на наличие уязвимостей. Для сокрытия действительного IP-адреса источника атаки такое ПО, в основном, задействует серверы, расположенные на территории США. Пятая часть атак исходит от российских IP-адресов.

Интересно отметить, что источником более трети атак на веб-приложения университетов являются внутренние злоумышленники (в среднем для сферы образования этот показатель равен 8%). Вероятно, это учащиеся, имеющие доступ к беспроводным сетям образовательного учреждения, а также доступ к локальной сети в учебных аудиториях.

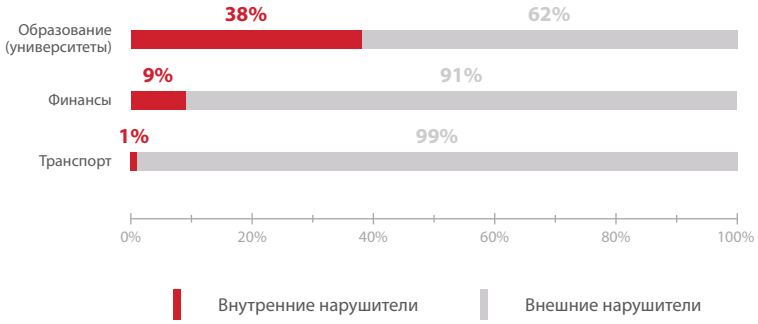

Рис. 10. Соотношение внешних и внутренних нарушителей

В финансовой сфере от внутренних нарушителей исходит около 10% атак. Не исключается также вариант, что нарушителем в ряде случаев может быть администратор системы, проводящий тестирование защитных механизмов.

Все обнаруженные события WAF должен анализировать на наличие корреляций между ними. Затем связанные события могут быть объединены в единую последовательность. Таким образом выявляются цепочки атак, которые могут состоять из множества действий, разделенных длительными промежутками времени. Эта функциональность WAF важна также и при выявлении целенаправленных атак или расследовании инцидентов. На рисунке ниже представлен пример обнаружения трех корреляционных цепочек PT AF, включая внедрение операторов SQL и атаки на отказ в обслуживании.

Рис. 11. Обнаруженные связанные события

В исследовании рассмотрены атаки, которые были подтверждены в рамках пилотных проектов с целью демонстрации эффективности работы PT AF.

Однако кроме атак, направленных непосредственно на веб-приложение, при соответствующих настройках параметров анализа событий PT AF способен выявлять другие классы атак, в том числе с целью эксплуатации уязвимостей ПО, например, нашумевших Shellshock, Heartbleed, HTTPoxy и др., а также фиксировать подозрительные события, которые могут являться попытками эксплуатации уязвимостей нулевого дня, информации о которых еще нет в открытом доступе.

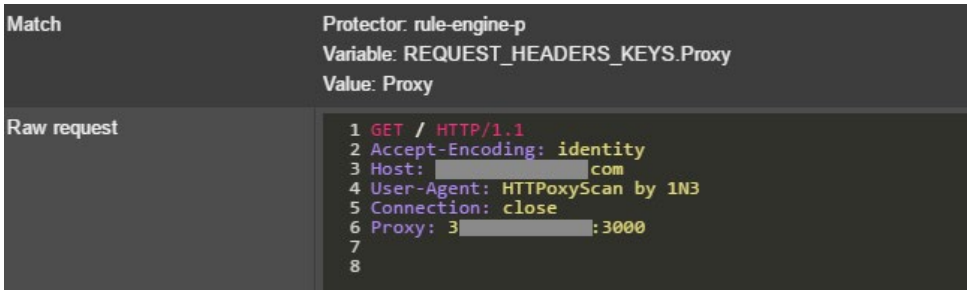

Рис. 12. Пример обнаружения попытки эксплуатации уязвимости HTTPoxy

Результаты работы PT Application Firewall на ресурсах Positive Technologies

Далее представлены результаты исследований на основе данных, собранных в ходе работы PT AF, который используется для защиты собственных веб-приложений Positive Technologies.

PT AF был настроен таким образом, чтобы выявлять цепочки атак на ресурсы Positive Technologies. Поэтому мы рассматриваем только связанные атаки, чтобы исключить недостоверные события. Также не учитывались атаки, которые осуществлялись специальным ПО для автоматизированного сканирования веб-приложения на наличие уязвимостей.

Распределение всех зафиксированных атак по степени риска показано на следующей диаграмме. Более половины составляют атаки высокой степени риска, 48% приходится на долю атак средней степени риска, атаки низкого уровня опасности в сумме составляют менее одного процента.

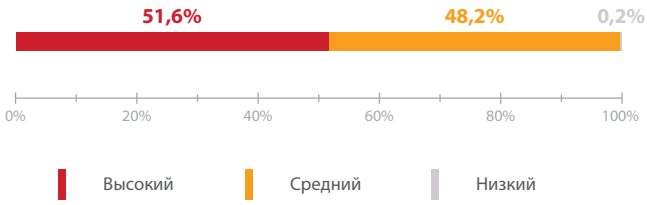

Рис. 13. Распределение атак по степени риска

PT AF выявляет корреляции между разрозненными атаками и при обнаружении связи выстраивает единую последовательность событий. На рисунках ниже приведен пример такой последовательности. В цепочку под общим названием SQLi-P multiply events объединено 10 атак высокой степени риска.

Рис. 14. Цепочка взаимосвязанных атак

EVENT_SEVERITY	EVENT_TAG	EVENT_DESCRIPTION	MATCHED_VARIABLE_NAME	TIMESTAMP
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.id	2016-09-27 03:14:56
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.id	2016-09-27 03:14:50
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.id	2016-09-27 03:14:47
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.id	2016-09-27 03:14:46
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.id	2016-09-27 03:14:45
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.id	2016-09-27 03:14:40
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.id	2016-09-27 03:14:40
high	SQL Injection	SQL injection attempt	REQUEST_GET_ARGS.id	2016-09-27 03:14:39

Рис. 15. Фрагмент списка взаимосвязанных атак

Все атаки из этой цепочки были совершены с турецкого IP-адреса.

Рис. 16. Источник цепочки атак

Около половины от общего числа атак на ресурсы Positive Technologies (45%) приходится на долю атак «Внедрение операторов SQL», что приблизительно соответствует показателю для отрасли IT, полученному в ходе пилотных проектов. Четверть от общего числа составили атаки «Подделка межсайтовых запросов», а пятую часть — «Неконтролируемое перенаправление». Пять процентов и менее составляют такие атаки, как «Межсайтовое выполнение сценариев», «Отказ в обслуживании» и «Удаленное выполнение кода и команд ОС». Другие атаки в сумме набирают 1%.

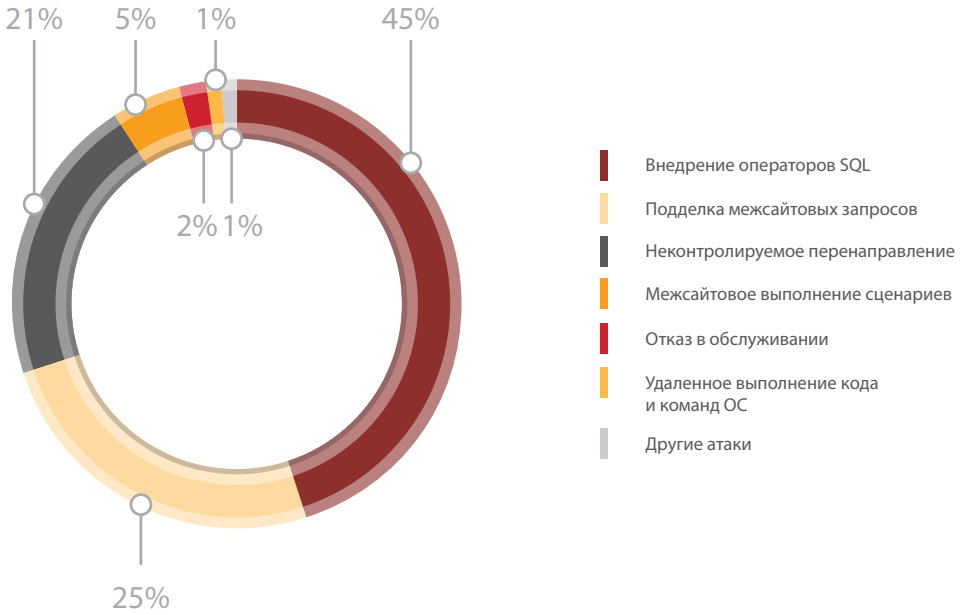

Рис. 17. Доли зафиксированных атак

Наибольшее число атак представляют собой попытки обхода средств защиты для несанкционированного доступа к веб-интерфейсу администрирования CMS, при этом некоторые злоумышленники действуют наугад, не зная точно, какая именно CMS используется, и предпринимают попытки обхода формы аутентификации, которая может быть расположена по разным адресам в зависимости от CMS.

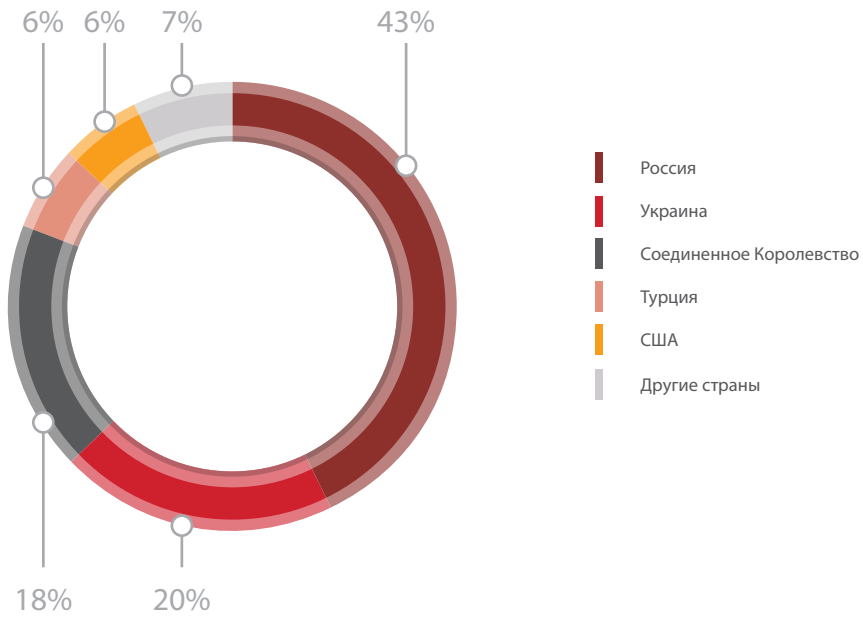

Рис. 18. Источники атак

Поскольку в этой части исследования рассмотрены ресурсы только одной компании, основные источники атак незначительно отличаются от результатов, полученных в ходе пилотных проектов: на первом месте находится Россия (43% атак), второе место занимает Украина (20% атак). Соединенное Королевство является источником 17% атак, что объясняется, с одной стороны, присутствием Positive Technologies на европейском рынке ИБ,

а с другой — использованием прокси-серверов провайдеров, зарегистрированных на территории королевства. Со стороны США и Турции зафиксировано по 6% атак.

При составлении графика атак по месяцам можно увидеть всплеск активности нарушителей в мае. Это связано с проведением международной конференции по информационной безопасности PHDays. Непосредственно перед конференцией и в дни ее проведения нарушители предпринимают попытки нелегальной регистрации для посещения конференции на сайте www.phdays.com или подделки результатов конкурсов. Такой вывод можно сделать, изучив характер атак в этот период. Преобладают попытки обхода средств защиты для несанкционированного доступа к веб-интерфейсу администрирования CMS, а также зарегистрировано большое количество внедрений операторов SQL на страницах, где публиковались результаты соревнований.

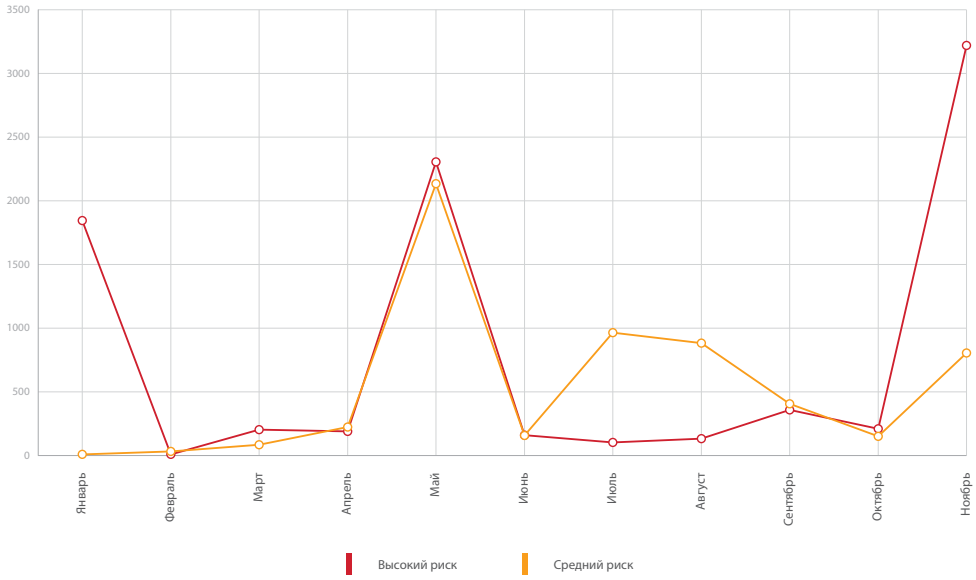

Рис. 19. Количество атак по месяцам

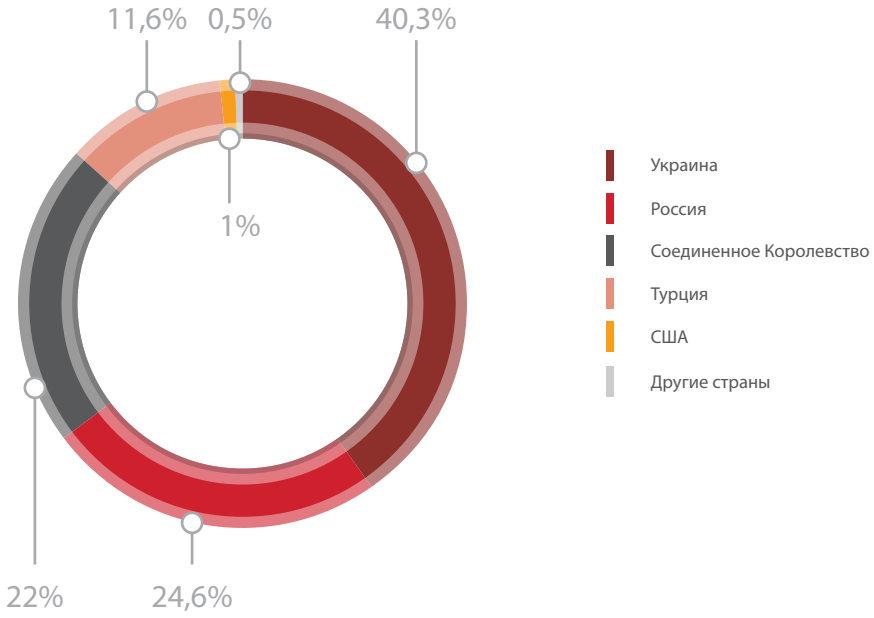

Рис. 20. Распределение источников атак в ноябре

Начиная с июля наблюдается постепенный рост числа атак на ресурсы Positive Technologies, стремительное увеличение количества атак происходит в ноябре. Кроме того, в ноябре возрастает доля атак со стороны Украины (40% от общего числа) и Турции (12%), в то время как активность злоумышленников из других стран, в том числе из России, колеблется незначительно. При этом растет процент атак высокой степени риска, в ноябре они составили 79% от общего числа.

Эти факты соотносятся с предупреждениями Федеральной службы безопасности о готовящихся кибератаках[1] на финансовую систему России. Спланированные массовые атаки с большой долей вероятности должны затрагивать не только непосредственно банковские системы, но и СМИ, в частности профессиональные порталы, которые могут быть использованы для распространения ложной информации от лица официальных представителей известных компаний или экспертов по безопасности. Кроме того, злоумышленники могут отрабатывать планируемые стратегии атак на сторонних ресурсах.

[1] http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10438041%40fsbMessage.html

Заключение

По результатам проведенных пилотных проектов и работы PT AF на ресурсах Positive Technologies можно сделать вывод, что большинство атак, совершаемых злоумышленниками, достаточно просты как в исполнении, так и в обнаружении средствами защиты, такими как WAF.

В то же время во второй половине 2016 года наблюдается значительный рост числа атак на веб-ресурсы, в первую очередь, с IP-адресов Украины и Турции. Принимая во внимание сообщения Федеральной службы безопасности о планируемых кибератаках, российским компаниям, в частности, финансовым организациям, рекомендуется заранее предпринять соответствующие меры для защиты критически важных компонентов и убедиться в эффективности используемых средств защиты.

Уровень технической подготовки и возможности злоумышленников, ставящих перед собой цель получить финансовую выгоду в результате атаки на веб-приложение, позволяют реализовать атаки высокого уровня сложности, в том числе требующие осуществления ряда, на первый взгляд, не взаимосвязанных действий.

Для выявления цепочек атак, в том числе в целях обнаружения длительных целевых атак и при расследовании инцидентов необходимо анализировать сотни событий и находить между ними корреляции, чтобы затем выстроить последовательную цепочку одного вектора атаки. Как показывают полученные результаты, PT AF справляется с обнаружением атак различных типов и уровней сложности, а также успешно выявляет векторы длительных многоступенчатых атак. Для эффективного предотвращения атак PT AF при обнаружении аномалий использует ряд защитных техник, например таких, как блокировка запроса к веб-приложению или ответа от веб-приложения, блокировка сессии пользователя или разрыв соединения, возможна блокировка IP-адреса злоумышленника с помощью встроенного межсетевого экрана, передача IP-адреса внешнему межсетевому экрану либо провайдеру. Кроме того, в PT AF реализовано взаимодействие с внешними системами сбора и анализа событий (SIEM) и оповещение средств защиты от DDoS сетевого уровня. Принимаемые меры позволяют своевременно останавливать атаки и защищать не только владельцев, но и пользователей веб-приложений.

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.

POSITIVE TECHNOLOGIES

ptsecurity.ru
pt@ptsecurity.com

facebook.com/PositiveTechnologies

facebook.com/PHDays