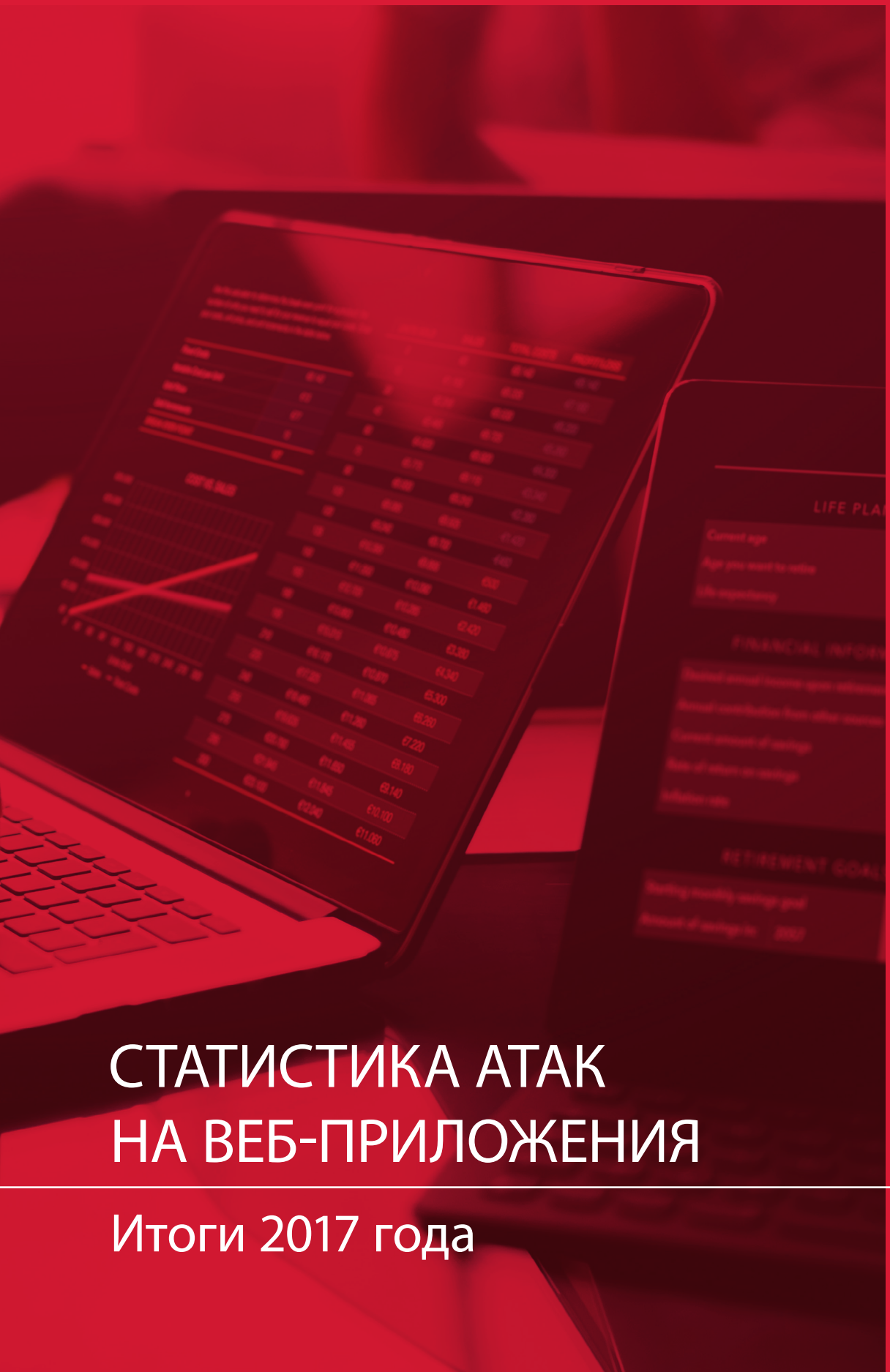
POSITIVE TECHNOLOGIES



СТАТИСТИКА АТАК НА ВЕБ-ПРИЛОЖЕНИЯ

Итоги 2017 года

СОДЕРЖАНИЕ

ТРЕНДЫ И ПРОГНОЗЫ

В течение 2017 года мы публиковали квартальные отчеты, посвященные атакам на веб-приложения. В текущем обзоре мы кратко подведем итоги 2017 года и расскажем о прогнозах на 2018 год.

Государственные учреждения. Все более популярными становятся атаки, в том числе и целевые, в ходе которых в качестве первичного источника заражения рабочих станций пользователей используются ресурсы сторонней компании. К таким ресурсам, в первую очередь, относятся официальные сайты государственных органов, которые имеют высокий уровень доверия среди посетителей, а следовательно, привлекательны для злоумышленников.

Государственные сайты всегда находятся под вниманием СМИ, поэтому преступники часто используют их для дефейса, чтобы привлечь к себе внимание.

В 2017 году мы видели успешные попытки повлиять на политическую обстановку путем проведения кибератак. В России в начале 2018 года мишенью хакеров стали веб-ресурсы, связанные с проведением президентских выборов. Мы также ожидаем волну атак на сайты, имеющие отношение к главному спортивному событию страны — финальной части чемпионата мира по футболу.

Банки и электронные торговые площадки. Атаки на пользователей все еще остаются самыми распространенными для веб-приложений финансовой сферы: злоумышленников привлекает возможность получения выгоды за счет клиентов онлайн-банков или различных платежных систем. Кроме того, веб-приложения — наиболее уязвимое звено в системе защиты самих банков, поэтому преступники продолжат атаковать банковские сайты с целью проникновения во внутреннюю инфраструктуру и кражи денег через банковские системы.

Всплеск популярности криптовалют и ICO, который пришелся на 2017 год, не обошел стороной и хакеров, активно использовавших уязвимости веб-приложений при атаках на ICO и криптовалютные биржи. Маловероятно, что в будущем году преступники откажутся от такого простого способа заработка.

Здравоохранение. Атаки в сфере здравоохранения нацелены прежде всего на получение доступа к данным пациентов для дальнейшего вымогательства или продажи на черном рынке. Кроме того, сайты медицинских учреждений, как и государственные, используются для заражения компьютеров посетителей вредоносными программами, например предназначенными для майнинга криптовалюты. Защита таких сайтов обычно находится на относительно низком уровне, что облегчает злоумышленникам задачу и провоцирует увеличение числа атак.

Образование. С внедрением информационных систем в образовательные процессы у недобросовестных учащихся появляются новые возможности исправить свою успеваемость — путем взлома электронных журналов, получения материалов экзаменов, внесения изменений в приказы о зачислении в вуз и пр. В прошедшем году мы уже видели примеры подобных атак и ожидаем роста их числа в будущем.

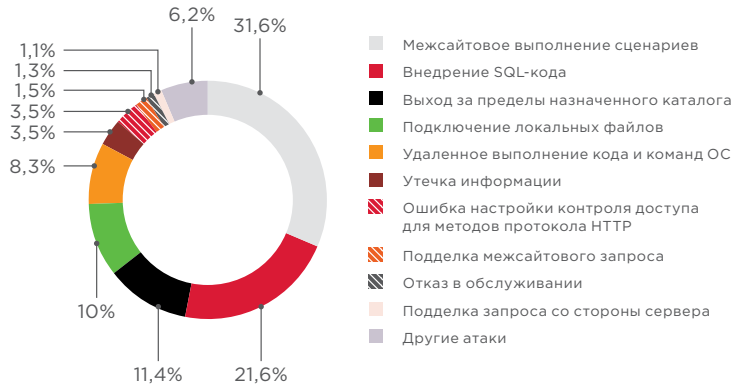
Энергетика и промышленность. В сфере энергетики и промышленности мы фиксировали сравнительно малое количество атак на веб-приложения, тем не менее они представляют особую опасность, поскольку характер атак говорит о высокой квалификации преступников и тщательно спланированных действиях. Мы ожидаем увеличения интереса злоумышленников к этим отраслям, что может выражаться не столько в количественном росте, сколько в использовании более сложных техник атак, выявить которые станет гораздо труднее.

Информационные технологии. Наибольшее число атак пришлось на веб-приложения компаний из сферы IT. Подобные атаки набирают популярность, поскольку позволяют нарушителям использовать доверенные веб-ресурсы в качестве базы для размещения своего вредоносного ПО или проводить иные атаки в отношении клиентов компании. Мы прогнозируем, что злоумышленники будут все чаще прибегать к такому способу распространения вредоносного ПО в массовых и целевых кибератаках.

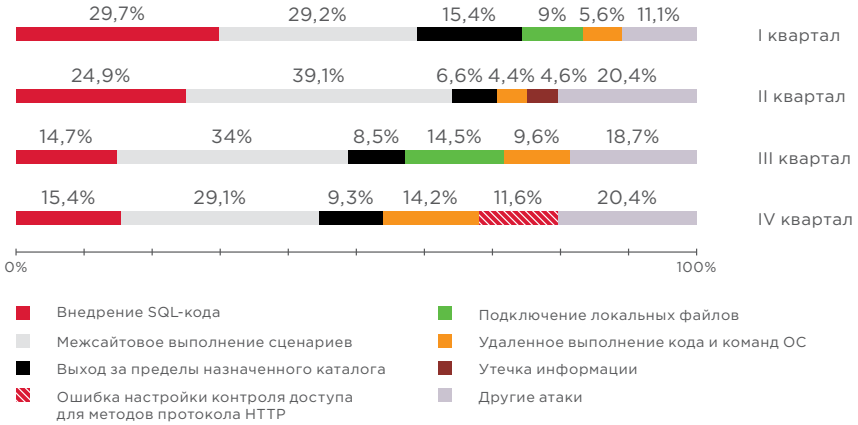
СТАТИСТИКА АТАК НА ВЕБ-ПРИЛОЖЕНИЯ

Типы атак

В течение всего 2017 года пятерка самых распространенных атак незначительно изменялась от квартала к кварталу. Среди наиболее популярных можно отметить атаки, направленные на пользователей веб-приложений, в частности атаку «Межсайтовое выполнение сценариев», которая составила почти треть от общего числа, и атаки, с помощью которых можно получить доступ к данным или выполнить команды на сервере, — «Внедрение SQL-кода», «Выход за пределы назначенного каталога», «Подключение локальных файлов», «Удаленное выполнение кода и команд ОС».



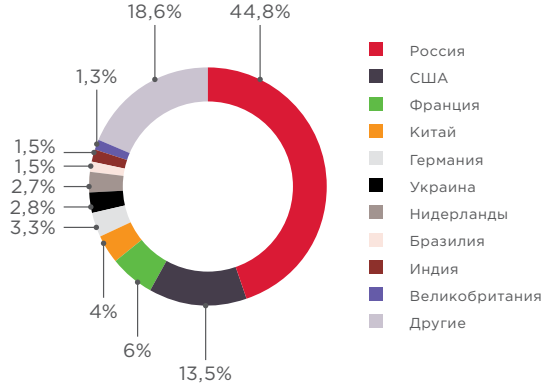
Топ-10 атак на веб-приложения



Изменения в топ-5 атак в течение года

Источники атак

Выявленные атаки осуществлялись преимущественно с российских IP-адресов. Это связано с тем, что большая часть пилотных проектов проводилась для российских компаний. В пятерку источников атак также вошли США, Франция, Китай и Германия.



Источники атак на веб-приложения

Статистика по отраслям

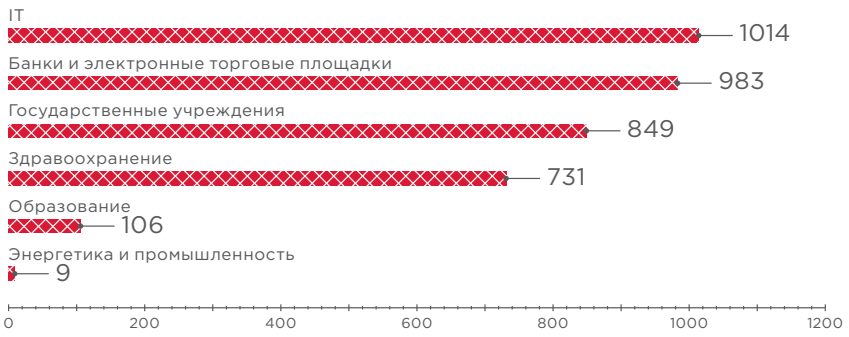
Среднее количество атак по отраслям

В 2017 году наибольшее число атак в день — более 900 — совершалось на веб-приложения IT-компаний и финансовых организаций (банков и электронных торговых площадок). Злоумышленников привлекает возможность получить прямую финансовую выгоду от компрометации банковских систем или в результате атак на пользователей. Атаки на сферу IT могут быть связаны с тем, что любая организация в той или иной степени пользуется услугами внешних подрядчиков для поддержания своих бизнес-процессов, поддержки внутренней инфраструктуры или внешних ресурсов. Доступ к IT-компании может открыть злоумышленнику возможность проникнуть в инфраструктуру множества компаний-клиентов. Так, в прошедшем году масштабная кибератака с использованием шифровальщика NotPetya началась со взлома компании, занимающейся разработкой бухгалтерского ПО.

Сайты государственных организаций и учреждения здравоохранения также вызывали интерес злоумышленников. В течение года мы наблюдали множественные взломы государственных сайтов как в политических целях, так и с целью заражения вредоносным ПО компьютеров обычных пользователей. В сфере здравоохранения резонансными оказались случаи утечки информации о пациентах и вымогательства денег за удаление данных.

Значительно реже злоумышленники атаковали сайты образовательных учреждений. Таким путем сложно получить большую прибыль, поэтому чаще всего виновными в атаках оказываются учащиеся, пытающиеся исправить свои оценки в электронных системах либо получить доступ к экзаменационным материалам.

Самыми немногочисленными оказались атаки на промышленные и энергетические предприятия — всего 9 атак в день на одну компанию. Целью таких атак главным образом является доступ к корпоративной сети, а преступники, проводящие их, обладают высокой квалификацией, поэтому тщательно продумывают свои действия и стараются действовать максимально незаметно, чтобы службы безопасности не обнаружили признаки целенаправленной атаки на раннем этапе.



Среднее число атак в день на веб-приложения одной компании

Рассмотрим, какие атаки были наиболее распространенными в отдельных отраслях и какие изменения происходили в течение 2017 года.

Государственные учреждения

Для государственных учреждений на протяжении всего года наиболее актуальными были атаки «Межсайтовое выполнение сценариев» и «Внедрение SQL-кода», составлявшие в совокупности более половины всех атак. Высокий процент атак, направленных на пользователей, по всей вероятности, связан с двумя факторами. Во-первых, среди посетителей государственных порталов высока доля людей, не обладающих глубокими знаниями об информационной безопасности, и злоумышленники могут легко заразить их компьютеры вредоносным ПО. Во-вторых, эти сайты могут являться промежуточным звеном в целевой атаке на другую компанию, сотрудники которой посещают официальный сайт государственного органа для решения рабочих вопросов. В результате компьютер пользователя может

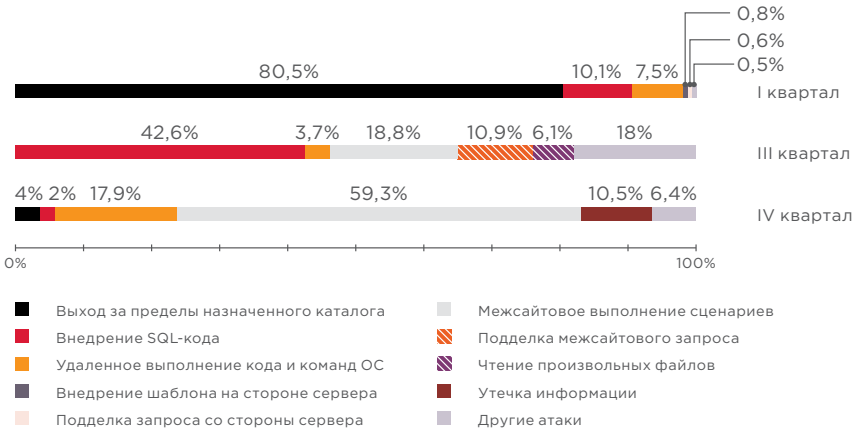
быть заражен с целью преодоления сетевого периметра и проникновения в инфраструктуру. В начале года была выявлена масштабная кампания, в ходе которой злоумышленники внедряли на сайты посольств и иных ведомств скрипт, заражающий устройства посетителей шпионским ПО, а позже с этой же целью был взломан сайт Национального совета США по внешней торговле.

Атаки на веб-ресурсы государственных структур совершаются и с политическими целями. Так, например, в России в 2018 году мишенью хакеров стали ресурсы, связанные с президентскими выборами. Государственные сайты могут использоваться для размещения провокационных материалов в ходе информационной войны: публикация ложных новостей, к примеру, на официальном сайте министерства иностранных дел может спровоцировать дипломатический скандал и осложнить внешнеполитическую обстановку. Похожая атака произошла в 2017 году в Катаре: преступники разместили сфабрикованные высказывания эмира, что вызвало резкое ухудшение дипломатических отношений с другими странами.

Топ-5 атак на веб-приложения госучреждений

Банки и электронные торговые площадки

В течение года на веб-приложения банков проводились атаки, целью которых являлось выполнение команд на сервере приложения («Внедрение SQL-кода», «Удаленное выполнение кода и команд ОС»). Таким образом злоумышленники пытались выявить недостатки защиты сетевого периметра, а как мы знаем из результатов исследований, именно уязвимости веб-приложений являлись единственным вектором проникновения во внутреннюю сеть банков во время работ по тестированию на проникновение. В четвертом квартале резко возросло число атак на клиентов банков «Межсайтовое выполнение сценариев»: это может быть связано с тем, что в конце года пользователи совершают больше операций.



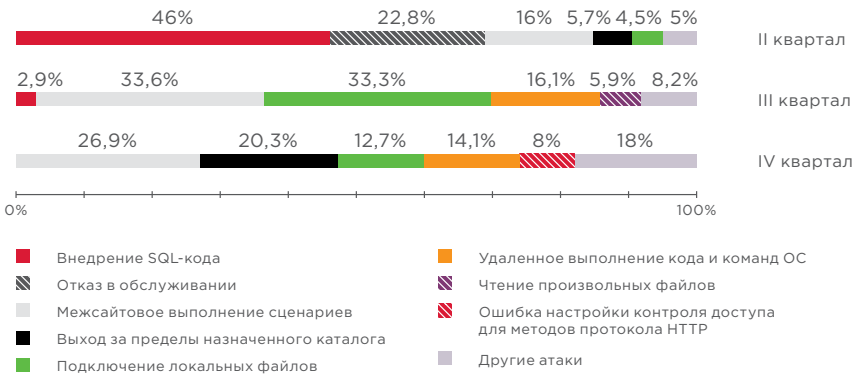
Топ-5 атак на веб-приложения банков и электронные торговые площадки

На 2017 год пришелся рост популярности криптовалют и ICO (initial coin offering, первичное размещение токенов), которые немедленно привлекли внимание хакеров. Большинство атак на криптовалютные биржи и площадки для проведения ICO были связаны с недостаточной защитой веб-приложений, например взломы проектов CoinDash и Enigma Project, в рамках которых преступники подменили на сайтах ICO адреса криптовалютных кошельков.

Здравоохранение

Злоумышленники, атакующие сайты в сфере здравоохранения, преследовали несколько целей. В течение года мы выявляли атаки, направленные на получение контроля над сервером или доступа к данным. В прошедшем году в СМИ неоднократно появлялась информация о фактах утечки данных о клиентах медицинских центров, за которыми следовало вымогательство денег с руководства клиник и непосредственно с пациентов. Например, можно вспомнить инцидент в литовской клинике пластической хирургии, когда хакеры опубликовали более 25 000 интимных фото пациентов до и после операций. Предварительно хакеры требовали за удаление данных выкуп в размере 344 000 евро у самой клиники и до 2000 евро — у отдельных пациентов. В октябре атаке подверглась клиника пластической хирургии в Великобритании, в результате чего хакеры завладели фотографиями клиентов, среди которых, как стало известно, были знаменитости и высокопоставленные лица.

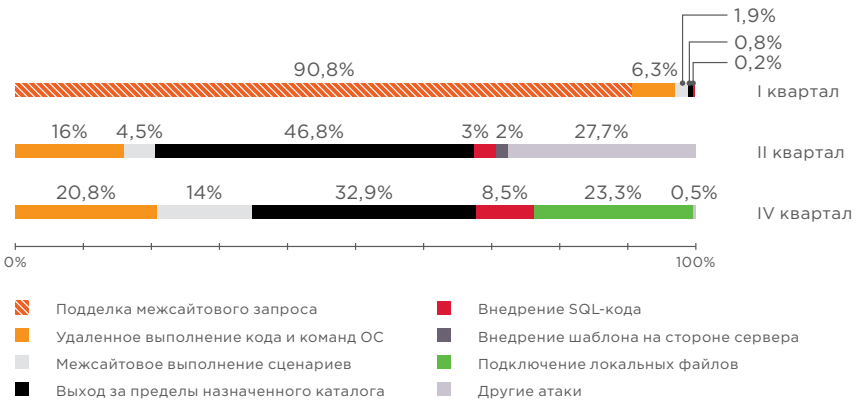
Сайты медицинских учреждений схожи с государственными в том плане, что уровень доверия к ним среди населения высок, но пользователи в большинстве своем не обладают познаниями в информационной безопасности, поэтому могут не заметить подозрительной активности на своем компьютере при посещении таких ресурсов. На протяжении всего периода исследования злоумышленники проводили атаки, которые позволили бы им внедрить вредоносный код на страницы сайта («Межсайтовое выполнение сценариев», «Удаленное выполнение кода и команд ОС», «Внедрение SQL-кода» и др.), чтобы заразить компьютер пользователя вредоносным ПО, направленным, в частности, на похищение банковских учетных записей или использование ресурсов процессора для добычи криптовалюты. Наглядный пример — обнаружение майнера криптовалюты Monero на сайте электронной регистратуры министерства здравоохранения Сахалинской области.



Топ-5 атак на веб-приложения в сфере здравоохранения

Образование

Во втором полугодии в сфере образования преобладали атаки, направленные на получение контроля над веб-приложением или сервером и на получение данных, в частности «Удаленное выполнение кода и команд ОС», «Выход за пределы назначенного каталога», «Внедрение SQL-кода». Атакующими, как мы заметили, являются чаще всего сами учащиеся, стремящиеся улучшить таким способом свою успеваемость. Уже становятся известны случаи взлома электронных дневников с этой целью, например инцидент в школе Новосибирска, когда школьник в течение месяца исправлял оценки себе и одноклассникам. На результаты, полученные в первом квартале, вероятно, оказал влияние небольшой объем выборки.

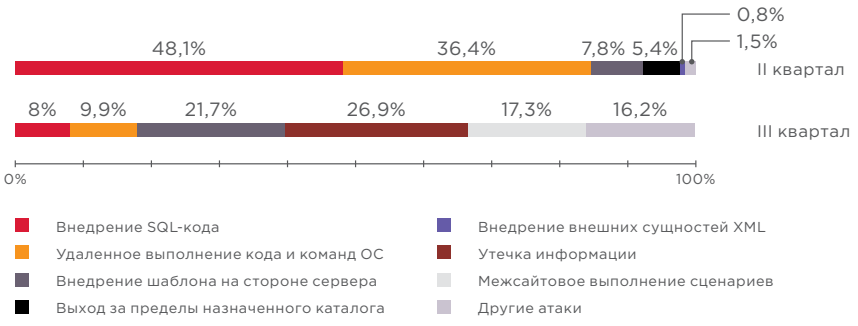


Топ-5 атак на веб-приложения в сфере образования

Энергетика и промышленность

Исследования для компаний из сферы энергетики и промышленности проводились во втором и третьем кварталах. За этот период были выявлены атаки, нацеленные в основном на выполнение команд на сервере приложения и частично на получение информации, которая может понадобиться для развития вектора атаки, — в том числе «Внедрение SQL-кода», «Удаленное выполнение кода и команд ОС», «Внедрение шаблона на стороне сервера». Целью преступников в данном случае является корпоративная (а затем и технологическая) сеть, получение доступа к техническим компонентам. Нарушения технологических процессов могут вызвать аварию на производстве и повреждение дорогостоящего оборудования, а следовательно, привести к затратам на восстановление промышленной инфраструктуры и недополучению прибыли либо к более серьезным последствиям (экологической катастрофе, человеческим жертвам).

С 2018 года вступил в силу федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», в соответствии с которым к объектам критической инфраструктуры могут быть, в частности, отнесены информационные системы предприятий из промышленной и энергетической отраслей. Организации, которым принадлежат такие системы, должны будут принять комплекс мер по обеспечению информационной безопасности, в том числе провести интеграцию в систему ГосСОПКА. Принятие этого закона свидетельствует о том, что правительство всерьез обеспокоено рисками, связанными с ростом числа кибератак на критические информационные ресурсы России.



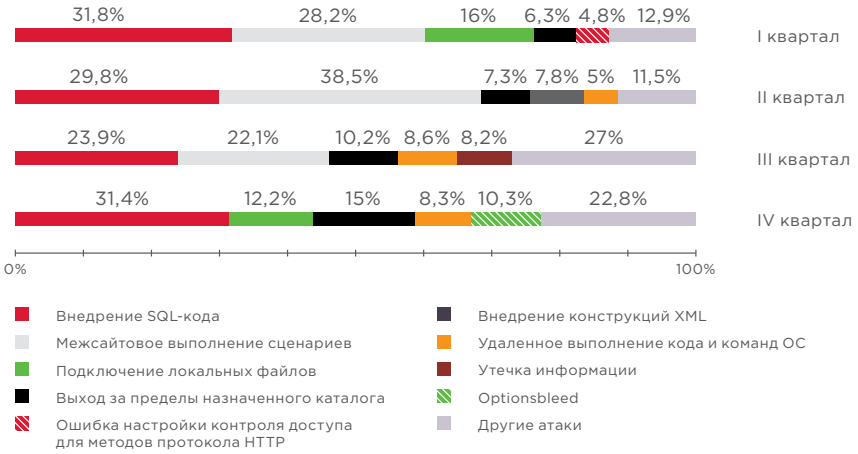
Топ-5 атак на веб-приложения в сферах промышленности и энергетики по кварталам

Информационные технологии

В IT-сфере на протяжении всех четырех кварталов значительную часть атак составляло «Внедрение SQL-кода», также были распространены атаки «Межсайтовое выполнение сценариев», «Подключение локальных файлов», «Выход за пределы назначенного каталога» и «Удаленное выполнение кода и команд ОС». Атаки на IT-компании мы прежде всего связываем с учащающимися случаями

компрометации ресурсов доверенных источников в целях широкого распространения вредоносного ПО. Например, в июне 2017 года прошла кибератака с участием шифровальщика NotPetya. Взлому подверглась компания, разрабатывающая бухгалтерское ПО, которое и послужило источником массового заражения. Осенью вредоносный код был обнаружен и в популярной утилите CCleaner на официальном сайте производителя. Использование ресурсов известной IT-компании (поставщика сетевого оборудования, ПО или услуг) для размещения своего вредоносного ПО или в качестве управляющего сервера выгодно злоумышленникам, поскольку соединения с IP-адресами этих компаний не вызывают подозрений у администраторов и службы безопасности. Помимо этого, злоумышленник может получить информацию, которая позволит проводить атаки в отношении клиентов компании, в качестве примера можно привести утечку информации с сервера Amazon Web Services.

В конце года в топ-5 вошла атака, эксплуатирующая уязвимость Optionsbleed (CVE-2017-9798). Примечательно, что первые попытки атак (в третьем квартале) были зарегистрированы всего через три часа после публикации детальной информации об этой уязвимости: такой короткий интервал практически не оставлял возможности принять меры для ее устранения.



Топ-5 атак на веб-приложения IT-компаний

ЗАКЛЮЧЕНИЕ

По итогам 2017 года мы видим, что злоумышленники активно атакуют веб-приложения, преследуя при этом разные цели: прямую кражу денежных средств, получение финансовой выгоды путем вымогательства, проникновение во внутреннюю инфраструктуру, политические цели, шпионаж и пр. Любое веб-приложение, даже не являющееся непосредственной целью киберпреступников, может подвергнуться атаке. Веб-ресурсы, владельцы которых не придают большого значения обеспечению информационной безопасности, легко могут стать орудием злоумышленников в массовой или целевой кибератаке.

Для обеспечения максимальной защиты веб-приложения следует проводить анализ защищенности, включая анализ исходного кода, на всех стадиях разработки, а также после введения в эксплуатацию, с целью выявления актуальных уязвимостей. Помимо этого, важно регулярно обновлять программные компоненты веб-приложения. Тем не менее и этих мер защиты может оказаться недостаточно, поскольку злоумышленники внимательно следят за публикациями о новых уязвимостях и стараются эксплуатировать их в кратчайшее время. По наших данным, минимальный промежуток между публикацией деталей уязвимости и первыми попытками ее эксплуатации составлял в ушедшем году всего три часа, а значит, разработчики ПО не всегда имеют возможность вовремя принять меры по устранению уязвимости и выпуску обновлений. Поэтому, чтобы эффективно противостоять преступникам, необходимо использовать дополнительные превентивные меры защиты, такие как межсетевой экран уровня приложений (web application firewall), для своевременного обнаружения и предотвращения атак на веб-ресурсы. Межсетевой экран должен не только обеспечивать противодействие известным атакам 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. Полезной функцией будет также взаимодействие с внешними системами сбора и анализа событий (SIEM) и оповещение средств защиты от DDoS сетевого уровня. Указанные меры позволят своевременно останавливать злоумышленников.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. 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.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com facebook.com/PositiveTechnologies facebook.com/PHDays