Ростелеком
Солар

Отчет об атаках на онлайн-ресурсы российских компаний

за 2022 год

Оглавление

Введение 3

Каким был DDoS 4

Количество и динамика 4

Ключевые характеристики 5

Какими были веб-атаки 5

Количество веб-атак 6

Ключевые характеристики 7

Заключение 8

Контакты 9

Введение

Минувший 2022 год изменил весь ландшафт киберугроз, а количество компьютерных атак выросло в разы. Сайты российских компаний с самого начала СВО стали ключевой мишенью хакеров. Последние активно использовали DDoS и веб-атаки, чтобы сделать онлайн-ресурсы недоступными для пользователей, нарушив таким образом работу компаний и организаций и посеяв панику в обществе. Хактивисты применяли дефейс, размещая на популярных сайтах провокационный контент.

Эксперты «Ростелеком-Солар» подготовили отчет о том, как киберпреступники использовали DDoS и веб-атаки в минувшем году. Аналитика составлена на основе данных об атаках, наблюдаемых ИБ-специалистами компании с января по декабрь 2022 года. Учтена информация о массовых атаках на магистраль, канальную инфраструктуру доступа к услугам, клиентское оборудование, а также веб-атаки на опубликованные в интернете онлайн-приложения организаций.

Для отчета была проанализирована информация почти о 600 компаниях из различных отраслей, включая телеком, ретейл, финансовый и государственный секторы. Все выявленные атаки были отражены специалистами «Ростелеком-Солар».

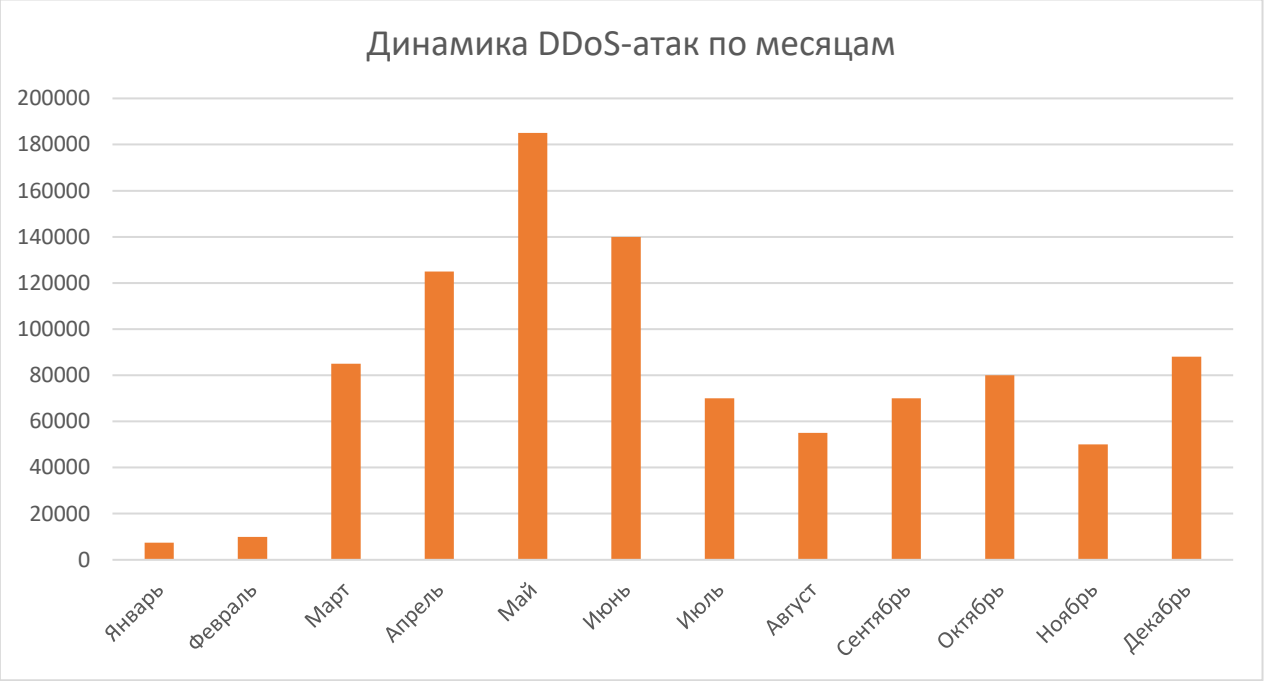
Каким был DDoS

В данной главе описаны атаки, зафиксированные и отраженные сервисом мониторинга трафика и защиты от DDoS-атак (Anti-DDoS). DDoS-атака – это действия злоумышленников, направленные на нарушение работоспособности инфраструктуры организации, ее порталов и веб-ресурсов. Хакеры искусственно создают множественные запросы к интернет-ресурсу, чтобы увеличить на него нагрузку и вывести из строя.

Количество и динамика

Традиционно самым атакуемым регионом стала Москва, так как именно здесь сконцентрирована большая часть организаций. На регион пришлось более 500 тыс. DDoS-атак. Далее следуют Уральский федеральный округ (почти 100 тыс. атак) и Центральный федеральный округ (чуть более 50 тыс. инцидентов).

Если говорить о динамике в целом по стране, то распределение атак по месяцам выглядит следующим образом:



На графике отчетливо виден многократный рост (почти **в 8 раз**) числа DDoS-атак в марте в сравнении с предыдущими месяцами года. Дальше динамика только нарастает, а пик подобных инцидентов приходится на май.

Это полностью коррелируется с общемировыми событиями. Еще 22-23 февраля эксперты «Ростелеком-Солар» отметили повышенную активность на хакерских форумах. А уже 25 февраля, после начала СВО, стали происходить массовые атаки на интернет-ресурсы госвласти. Наряду с этим трендом в марте начался заметный рост атак на бизнес и в первую очередь на банковский сектор. Географически большая часть атак в начале марта шла с IP-адресов, зарегистрированных в США.

Пик атак в мае, скорее всего, связан с празднованием Дня Победы. Хактивисты пытались «забить» мусорным трафиком каналы связи ресурсов, имеющих отношение к праздничным и патриотическим мероприятиям.

Далее видно, как DDoS-активность постепенно снижается. К 3 кварталу наши эксперты действительно фиксировали спад массовых атак и переориентацию злоумышленников на более сложные целевые удары. DDoS же скорее отыграл аномальный рост первой половины года и вернулся к более стандартным значениям. Однако число подобных атак все равно превышает средние показатели предыдущих лет. А значит, угроза остается актуальной.

DDoS-атака в случае ее успешности может нанести серьезный удар по организации. Например:

- клиенты, не получив доступа к сайту, могут перейти к конкурентам, а сам сайт на время пропадет из поисковой выдачи;
- могут быть атакованы не только публичные ресурсы, но и непубличные, которые используют сотрудники для работы (парализована почта или удаленный доступ к рабочему месту), что приведет к нарушению бизнес-процессов;
- хакеры часто атакуют ресурсы, являющиеся основным инструментом бизнеса, что может привести к серьезным потерям (например, внутренние банковские ресурсы, которые отвечают за транзакции и т. п.);
- хакеры могут потребовать крупный выкуп, чтобы прекратить DDoS-атаку на сайт жертвы;
- простая DDoS-атака может стать дымовой завесой для более серьезного инцидента, и пока ИБ-специалисты пытаются восстановить работу сервера, хакеры могут похитить конфиденциальные данные клиентов или корпоративную информацию.

Ключевые характеристики

760 Гбит/с

составила самая мощная атака 2022 года

Основной поток DDoS-атак не отличался высокой мощностью: они не превышали 50 Гбит/с. Но в то же время стало больше мощных целевых атак на конкретные компании или массированных ударов, приуроченных к каким-то конкретным событиям. В феврале (сразу после начала СВО) мы зафиксировали атаку более 760 Гбит/с, что почти в 2 раза превышает самую мощную атаку предыдущего года.

Длительность большинства атак также была невысокой, но некоторые оказались рекордными по продолжительности. В частности, одна из зафиксированных экспертами «Ростелеком-Солар» DDoS-атак длилась 2 000 часов, то есть почти 3 месяца.

3 месяца

длился самый продолжительный DDoS

Какими были веб-атаки

В данной главе описаны атаки, отраженные сервисом защиты веб-приложений (Web Application Firewall, WAF). Веб-атаки направлены на логику самого приложения, когда злоумышленники пытаются использовать уязвимости, которые есть на сайте. Сервис WAF обеспечивает защиту веб-ресурсов заказчика от атак уровня L7 (то есть расширенная защита от DDoS-атак уровня приложений и атак из списка OWASP Top 10, включая SQL-инъекции, межсайтовый скриптинг, незащищенность критичных данных и т. д).

Количество веб-атак

Согласно квартальным отчетам «Ростелеком-Солар», в 1 квартале года почти 80% критических киберинцидентов было связано именно с атаками на онлайн-ресурсы российских организаций, а ко 2 кварталу эта доля превысила 92%.

Статистика подтверждается и активностью наших клиентов. За один только март запросов на услуги защиты веб-приложений было почти **на 30% больше**, чем за весь предыдущий год. В итоге за неполный 2022-й мы подключили к сервису WAF (Web Application Firewall) в три раза больше заказчиков, чем в 2021 году в целом. Причем больше половины в этот момент уже находились под атакой.

21,5 млн инцидентов

с высокой степенью критичности зафиксировал WAF

Наибольшее число (**30%**) веб-атак было направлено на госсектор. Его атаковали как минимум в три, а местами и в 12 раз чаще, чем в прошлом году. Эта отрасль всегда была в фокусе внимания хакеров: недоступность госресурсов, когда люди не могут увидеть важную информацию или получить услугу, создает нервное напряжение в обществе, а дефейс таких порталов вызывает не только раздражение и панику пользователей, но и имиджевые потери госвласти в целом. Кроме этого, веб-уязвимости позволяют получить доступ к базам данных приложений, в которых могут содержаться персональные данные пользователей госпорталов либо иная конфиденциальная информация о гражданах. Также существует вероятность несанкционированного доступа к ключевым функциям таких систем, что может вызвать широкий общественный резонанс.

Также четверть веб-атак была направлена на финансовый сектор. Традиционно привлекательная для злоумышленников сфера показала кратный рост по атакам на онлайн-ресурсы – в два-четыре раза. Недоступность подобных веб-приложений также крайне чувствительна для пользователей. В то же время взлом сайта может привести хакеров к базам данных, в которых содержатся финансовая информация или персональные данные клиентов.

На третьем месте оказались образовательные учреждения – на них приходится **16%** веб-атак. В основном атакам подвергались учреждения высшего образования, а действия хакеров могли быть связаны с попытками помешать проведению приемных компаний.

Ключевые характеристики

Ниже разберем самые популярные типы зафиксированных в отчетном периоде веб-атак и уязвимостей, которые используют злоумышленники для вредоносных действий. В статистке учитываются DDoS-атаки прикладного уровня, веб-атаки и уязвимости, которые могли привести к инцидентам с высокой степенью критичности.

DDoS-атаки уровня приложений

Большая часть атак, отраженных WAF, – это атаки типа отказ в обслуживании, то есть DDoS. DDoS бывает двух типов: уровня сети, когда хакеры «забивают» канал связи или нагружают сетевое оборудование, и уровня приложений, когда мусорные запросы выводят из строя опубликованный веб-сервис. В первом случае помогает магистральный Anti-DDoS (результаты работы сервиса описаны выше). От более специфичного DDoS – уровня приложений (уровня L7) – защищает сервис WAF.

OS Commanding

Это веб-уязвимость, которая позволяет злоумышленнику выполнять произвольные команды операционной системы на сервере, где выполняется приложение. При успешной эксплуатации подобной уязвимости злоумышленник может полностью скомпрометировать приложение и все его данные. Попытки подобных атак мы видели в отношении нескольких ведомств, крупных госкомпаний и региональных банков.

Path Traversal

Реализуя атаку обхода пути (Path Traversal), злоумышленник может получить несанкционированный доступ к различным данным системы, включая учетные данные внутренних серверов, файлы и библиотеки операционной системы и т.д. Для этого хакеры внедряют в атакуемую систему параметры, которые дают возможность манипулировать путями файлов, вовлечённых в операции бэкенда. Подобные атаки становятся возможными из-за недостаточной проверки обрабатываемых программой команд. Помимо госсектора, где хакеры пытались использовать эту уязвимость, WAF блокировал подобные атаки в отношении нескольких вузов, производственных организаций, компаний из отрасли финансов и фармацевтики.

Local File Inclusion

Уязвимость исполнения локальных файлов (Local File Inclusion) позволяет злоумышленникам через браузер запускать локальные файлы на сервере. С помощью специально сформированного запроса хакер может получить доступ в том числе и к конфиденциальной информации. Уязвимость возникает, когда веб-приложение ссылается на файл в локальной файловой системе, а не в безопасном удаленном месте. Попытки подобных атак мы фиксировали в отношении федеральных и региональных органов власти, нескольких госкомпаний, ряда банков и страховых организаций.

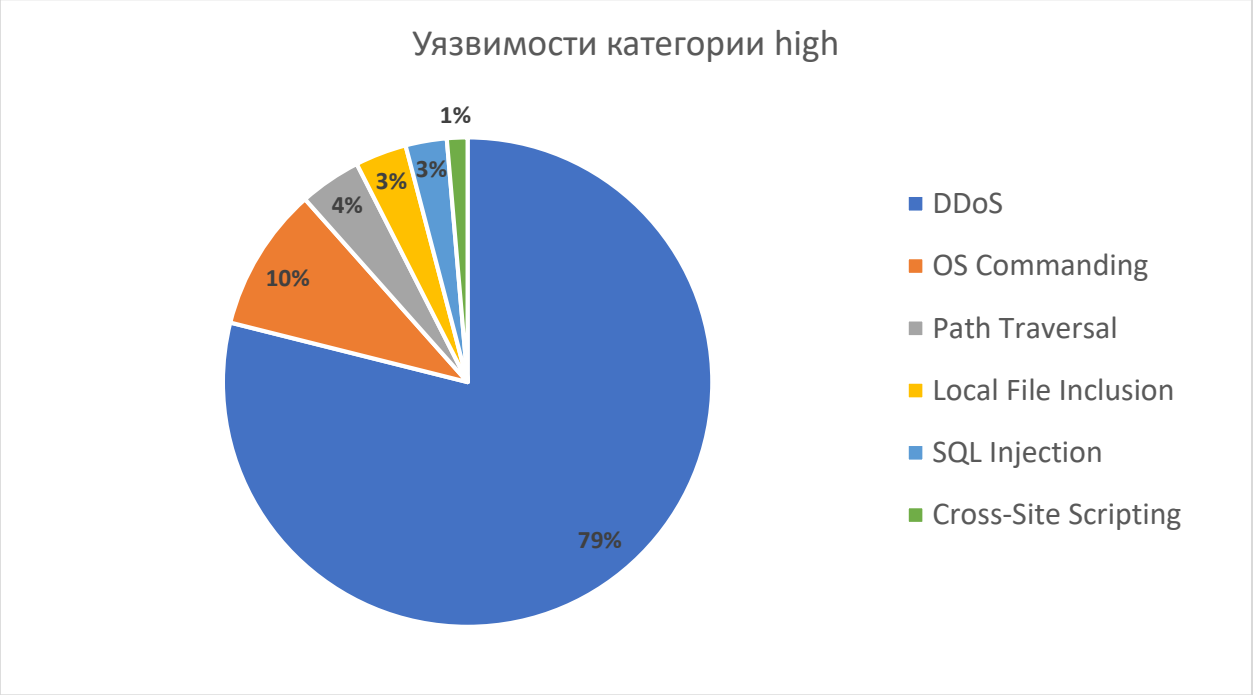
SQL Injection

Внедрение SQL-кода – это один из самых распространенных способов взлома сайта, который мы встречали в абсолютно разных отраслях (госсектор, финансы, производство, образование, телеком и проч.). Уязвимость возникает из-за недостаточной проверки вводимых пользователем команд, что позволяет модифицировать запросы к базам данных. В итоге злоумышленник получает доступ к закрытым и конфиденциальным данным.

Cross-Site Scripting

XSS или «межсайтовый скриптинг» также является весьма распространенной уязвимостью, которая часто встречается в веб-приложениях. Благодаря ей злоумышленник может внедрить на страницу код, который не предусмотрен разработчиками. И когда пользователи будут заходить на страницу, будет выполняться сценарий, внедренный хакерами. Таким образом, последние могут незаметно

перенаправить жертву на фишинговую страницу, получить учетные данные пользователей и даже администратора, что фактически дает полный контроль над сайтом. Эта уязвимость также встречается в веб-приложениях организаций из разных отраслей.



Заключение

- После начала СВО был зафиксирован очевидный всплеск атак на онлайн-ресурсы. Злоумышленники атаковали каналы связи и инфраструктуру как на сетевом и транспортном уровне, так и обращались к уязвимостям веб-приложений в рамках более изощрённых атак.

- За отчетный период была зафиксирована рекордная по мощности и продолжительности DDoS-атака. Однако в целом хакеры вели «ковровые бомбардировки» несложными и массовыми атаками. При атаках на веб злоумышленники продолжали эксплуатировать известные уязвимости и дыры в безопасности, многие из которых имеют высокую степень критичности и могут привести к полному контролю хакеров над приложением и краже данных пользователей.

- Конец года компенсировал резкий всплеск первых двух кварталов – злоумышленники сконцентрировались на целевых более сложных атаках на конкретные компании и отрасли. При этом уровень сетевых атак остается высоким и превышает средние показатели предыдущих лет, поэтому угроза остается актуальной.

Контакты

rt.ru

rt-solar.ru

solar@rt-solar.ru

+7 (499) 755-07-70