DDOS-GUARD

Итоги 2015 года

111 Количество мощных атак (свыше 100 Гбит/сек.)

на 5% больше (округленно) Мощных атак, чем в прошлом году

12 Количество мегамощных атак (свыше 200 Гбит/сек.)

в 4 раза Выросло количество мега-мощных атак, по сравнению с прошлым годом

1,37 Гбит/сек. Средняя мощность атак

в 1,5 раза Выросла средняя мощность

242 Гбит/сек. Самая мощная атака. Это на 36% мощнее рекорда 2014 года

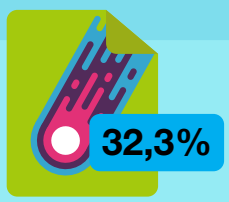
Если говорить про пакетные атаки, то рекорд 2015 года - атака с пиком 47,3 млн пакетов в секунду, что на 16% меньше, чем в 2014 году. Что, однако, не позволяет говорить об общем ослаблении волюметрических атак, как отмечают специалисты DDoS-GUARD. Среднее значение - 6,5 тыс. пакетов в секунду - выросло по сравнению с прошлым годом на 3%.

14321 атака

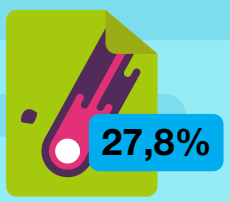
Была зафиксирована за самый “горячий” квартал (январь, февраль, март)

6102 атаки

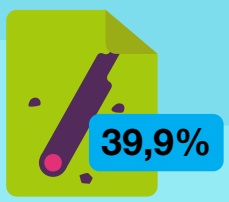
Самый насыщенный атаками месяц - январь



TCP



UDP

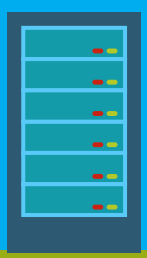


Другие

Соотношение количества атак по типам сохранилось на уровне 2014 года

Рейтинг “жертв” (по процентному соотношению количества атак)

21,5% Хостинги



18% Игровые проекты

16,9% Торрент-трекеры

16,7% СМИ

15% Интернет-магазины

11,9% Другое

Количество атак за 2015 год

50146
DDoS-атак за год

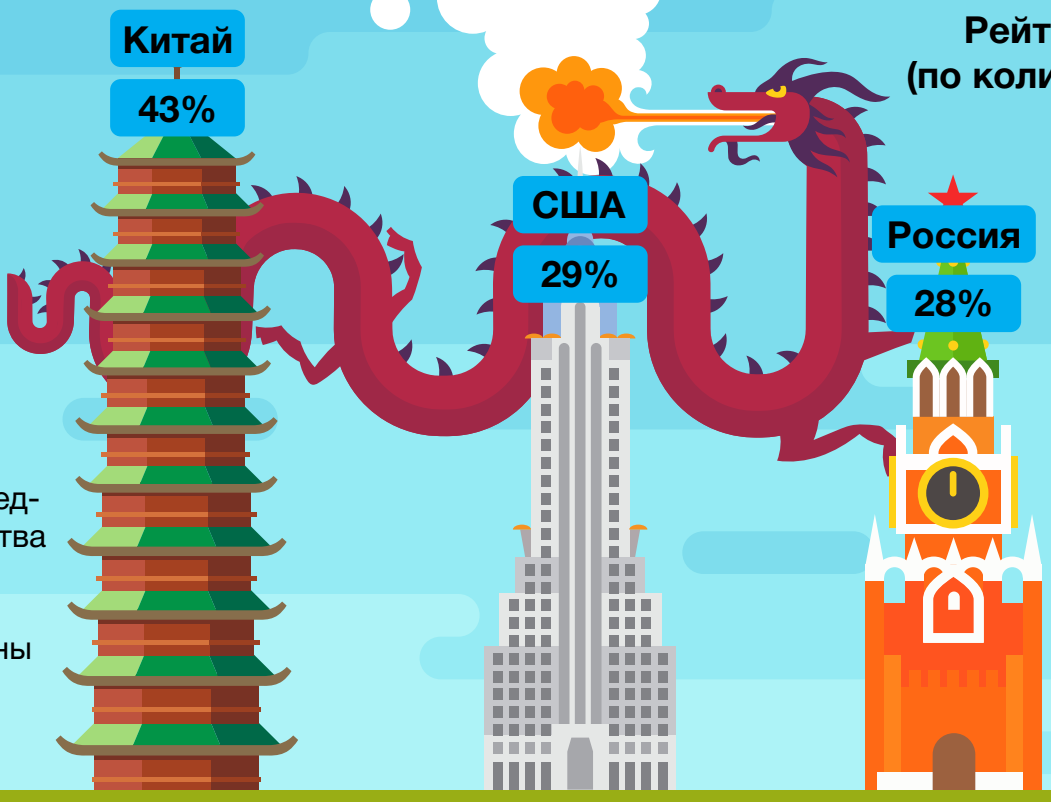
137
атак в день (в среднем)

5
атак в час (в среднем)

Общие тенденции

Кратковременный UDP-флуд становится все мощнее. Но понимая, что он не проходит через фильтры системы защиты, хакеры ищут новые способы заблокировать ресурс жертвы, используя для организации потока паразитного трафика устаревшие и малоизвестные протоколы Интернета, а также комбинируя продолжительные атаки средней мощности с короткими супермощными всплесками.

Рейтинг стран (по количеству атак)



Рассчитано исходя из среднего количества атак на 1000 ресурсов из каждой страны за год

Бессменным лидером в данном рейтинге на протяжении четырех лет работы DDoS-GUARD остается Китай, а Россия поменялась местами с Канадой, которая занимала третье место в 2014 году.

Стоит отметить, что DDoS-GUARD обслуживает большое количество клиентов как из упомянутых стран, так и из Европы, Южной Америки и Азии, поэтому статистика может считаться общемировой.

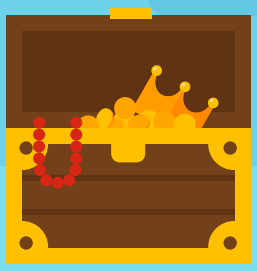
Необычные атаки

В 2015 году были зафиксированы единичные атаки по протоколам IPSec и RIPv1. IPSec - протокол, используемый для передачи зашифрованных данных и организации работы виртуальных туннелей.

RIPv1 - устаревший протокол маршрутизации, по которому работают роутеры старых моделей. Его используют для усиления ddos-атак типа DNS, SSDP. RIPv1 - привлекательный ресурс для организации DDoS-атак. Большинство источников — маршрутизаторы старых моделей, годами работающие в жилых домах или офисах.

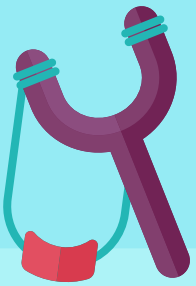
Но система фильтрации DDoS-GUARD справилась с этими атаками, сохранив доступность ”жертв”.

Мотивы злоумышленников



Корыстные. Хакеры использовали шантаж, требуя от клиента DDoS-GUARD выкуп за предотвращение ddos-атаки, который превышает по сумме стоимость защиты. Однако для уже защищенного ресурса такие атаки прошли незамеченными (пиковая мощность составила всего лишь 24 Гбит/с) , система защиты беспроблемно их отфильтровала.

Якобы общественно-политические. Так называемые хактивисты в 2015 году заявили в соцсетях и через интернет-СМИ, что ddos-атаки, организуемые на торрент-трекеры - это средство борьбы с пиратством в сфере контента. Речь идет о группировке OfcTeam и их атаках на Rutracker.org. После подключения трекера к системе защиты, стабильная работа ресурса была восстановлена. Кроме того, поступали угрозы от некой Антипирасткой коалиции, однако они не были реализованы.



В целом же, хакеры в ушедшем году не смогли удивить технической сложностью атак, но при этом стали действовать более публично, обращаясь к потенциальным жертвам и их защитникам с угрозами и заявлениями через социальные сети.

Прогноз

Рост мощности флуда, дальнейшие поиски хакерами новых уязвимостей, увеличение числа атак на уровне приложений, реализация комбинированных ddos-атак (мощный флуд плюс атаки на приложения).

О нас

DDoS-GUARD - лицензированный оператор связи-провайдер защиты от ddos-атак.

Обслуживает клиентов со всего мира. Емкость собственной георасперделенной сети - 1,5 Tbps.

Данные, представленные в отчете, собраны автоматической системой статистики, разработанной специалистами DDoS-GUARD.