Qrator Labs: статистика DDoS-атак в 2013 году и прогноз на 2014 год

Москва, 4 марта 2014 г. — Компания Qrator Labs, специализирующаяся на защите сайтов от DDoS-атак, составила отчет по активности киберпреступников в этой сфере в 2013 году.

За прошлый год компания **Qrator Labs** с помощью собственного одноименного сервиса нейтрализовала 6 644 DDoS-атак. Годом ранее эта цифра составила 3 749. Рост обусловлен как увеличением числа клиентов **Qrator Labs**, так и ростом активности киберпреступников в целом.

По словам Александра Лямина, основателя и Генерального директора **Qrator Labs**, показатели компании отражают тенденцию отрасли: «По нашим оценкам, общее количество атак на российские сайты выросло за прошлый год примерно на четверть. Также возросло среднее число атак, приходящихся на один сайт. Одна из причин происходящего — в том, что осуществить DDoS-атаку в последние годы не становится сложнее. Например, для организации атаки типа DNS Amplification полосой 150 Гб/сек и больше достаточно 5-10 серверов средней мощности».

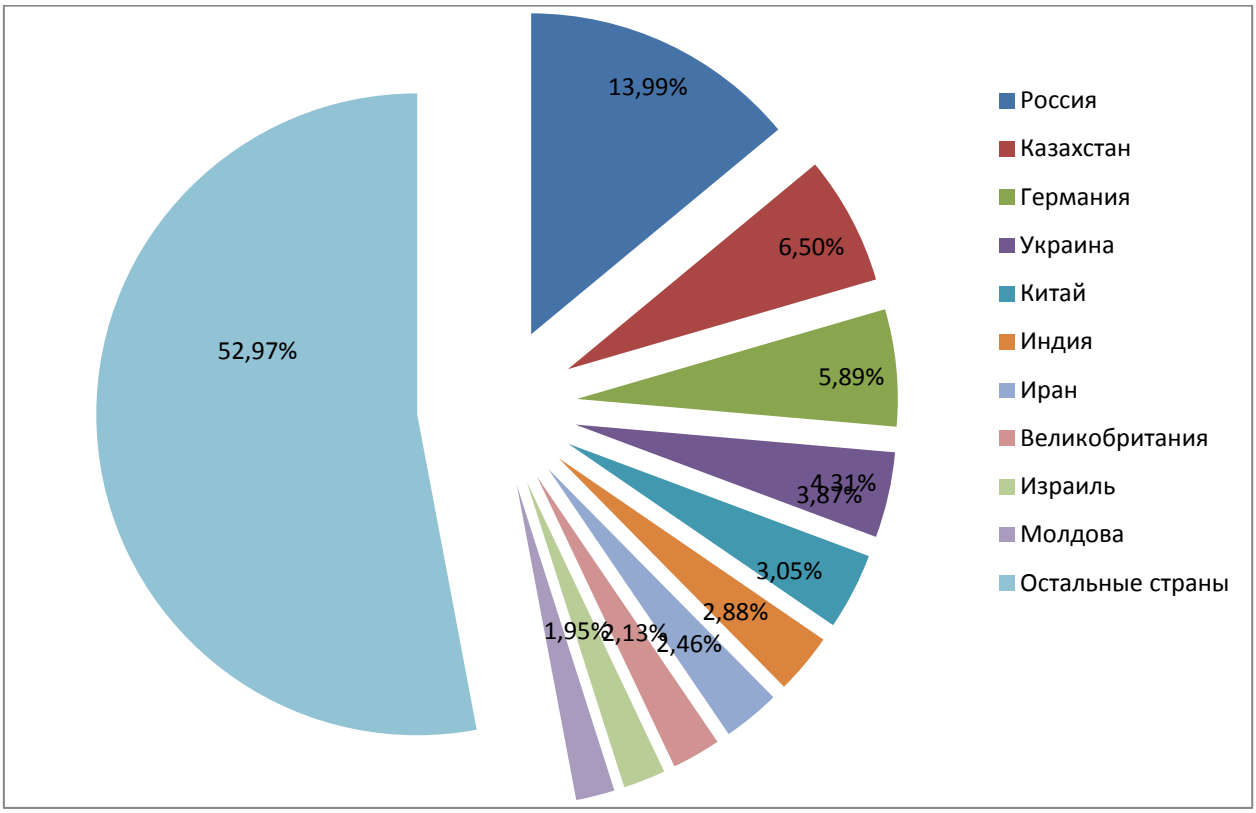

Рис. 1. Количество ботов в различных странах мира, по данным Qrator Labs

По сравнению с предыдущим 2012 годом, в 2013 году максимальное число атак в день, нейтрализованных сетью фильтрации трафика **Qrator**, возросло с 73 до 151.

Максимальный размер ботнета, задействованного в атаке, вырос с 207 401 до 243 247 машин. Увеличилась также доля Spoofing-атак – с 43,05% до 57,97%. Это атаки, в которых вместо IP-адреса реального пользователя подставляется фальшивый.

Максимальная длительность атаки сократилась с 83 дней в 2012 году до 22 дней в 2013, а уровень средней доступности WEB-ресурсов компаний, пользующихся услугами сети Qrator, вырос с 99,71% до 99,83%.

«Хакеры стали более гибкими в отношении выбора метода атаки. Мы наблюдаем четкую тенденцию уменьшения длительности атак на наших клиентов — если раньше исполнители атак могли долго пытаться преодолеть защиту, то сейчас речь идет в основном о кратковременных «пробах прочности», за которыми следует отказ от намерений либо смена методики или технологии атаки», — говорит Александр Лямин.

По данным **Qrator Labs**, на фоне заметного роста «интеллектуализации» ботнетов, имитирующих поведение рядового пользователя, также существенно выросло количество высокоскоростных атак типа SYN-flood.

Число атак в 2013 году увеличилось также в среднем на одного клиента сети Qrator. Такая тенденция уже наблюдалась в 2012 году по сравнению с 2011, однако в 2013 году темпы роста увеличились в два раза – с 17% до 34%.

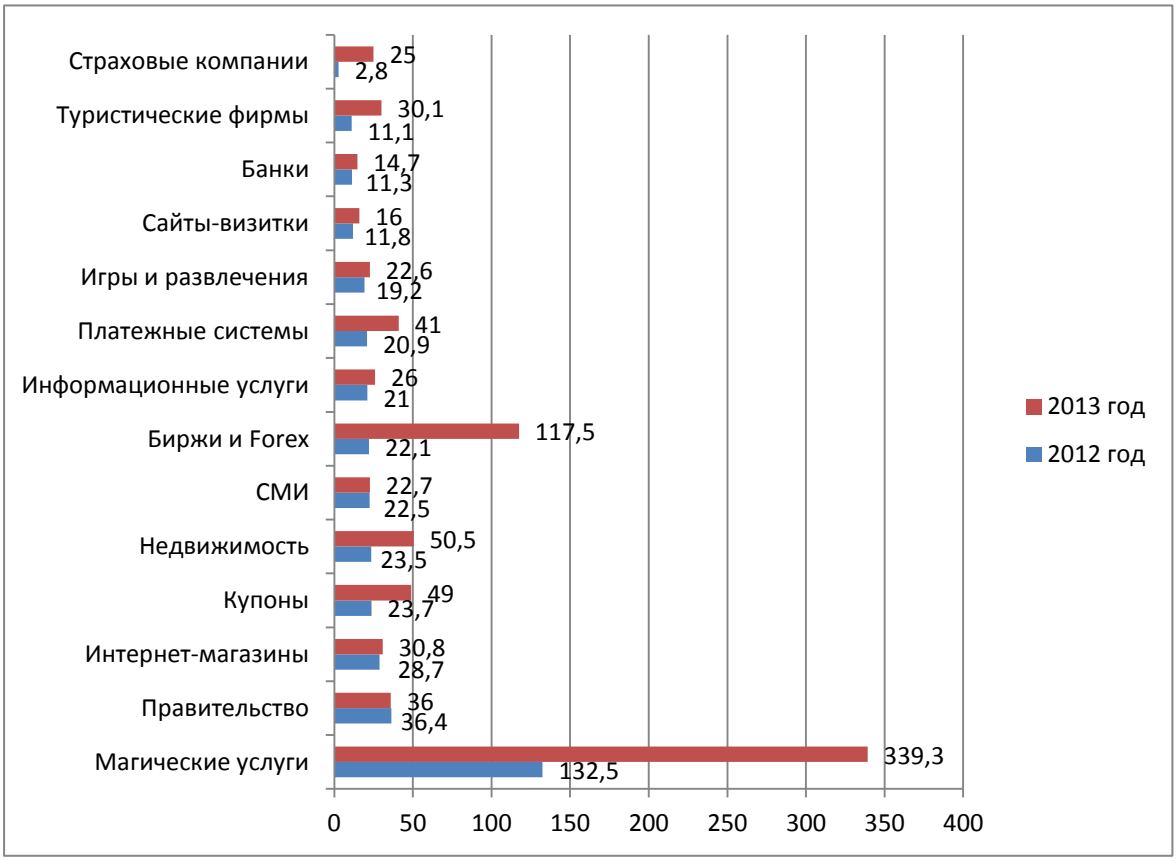

Рис. 2. Среднее количество атак на одного клиента Qrator Labs в год

С марта по октябрь 2013 года подавляющее число атак производилось с использованием DNS Amplification. Это атаки, когда злоумышленник посылает запрос (обычно короткий в несколько байт) уязвимым DNS-серверам, которые отвечают на запрос уже в разы большими по размеру пакетами. Если при отправке запросов использовать в качестве исходного IP-адреса адрес компьютера жертвы (ip spoofing), то уязвимые DNS-серверы будут посылать ненужные пакеты этому компьютеру, пока полностью не парализуют его работу. Часто объектом такой атаки оказывается инфраструктура провайдера, которым пользуется жертва. Нападения такого типа совершались в прошлом году как на клиентов крупных операторов, так и небольших провайдеров хостинговых услуг.

С октября по декабрь проявила активность крупная бот-сеть, объединяющая более 700 тысяч компьютеров-зомби, которая использовалась для нападения преимущественно на российские банки среднего размера. Эта активность совпала с действиями ЦБ РФ по отзыву лицензий у ряда банков.

В декабре 2013-го стало расти число атак с использованием технологии NTP Amplification. Такие атаки по принципу организации похожи на DNS Amplification, но вместо DNS-серверов злоумышленники используют серверы синхронизации времени -- NTP. Увеличение количества подобных инцидентов продолжается и в первые два месяца 2014 года.

С учетом приведенной статистики можно сказать, что в 2013 году наблюдался ряд тенденций, которые в 2014 году продолжат свое развитие:

- Рост числа высокоскоростных атак с использованием Amplification публичных UDP-сервисов;
- совершенствование атак уровня приложений с использованием ботнетов. Такие атаки часто низкоскоростные и алгоритмы их автоматического обнаружения довольно сложны;
- цель 2013 года у киберпреступников — DNS-серверы; технология DDoS года — DNS Aplification.

«В 2014 году ситуация с DDoS в Рунете будет зависеть от того, как отреагирует сообщество операторов на вызовы киберпреступников. Два года назад ожидалось, что атаки сетевого уровня будут постепенно уступать место прикладным атакам, но летом 2013 года преступники смогли организовать атаку 150 Гб/сек, и это не повлекло никакой реакции в индустрии. Следовательно, если не будут предприниматься согласованные меры всех участников межоператорского взаимодействия по противодействию угрозе, с высокой вероятностью можно ожидать устойчивого роста и скоростей, и количества атак», — продолжает Александр Лямин.

Другим важным трендом на ближайшие годы могут стать атаки с использованием протокола BGP, отвечающего за глобальную доступность сетей в Интернете (так называемые атаки BGP Hijacking). Суть проблемы заключается в отсутствии механизмов

проверки источника маршрутной информации, что в результате делает возможным неавторизованное перенаправление трафика (перехват) на свою AS и его последующий анализ или сброс. Обнаружить такой перехват со стороны атакуемой AS теоретически невозможно. До 2013 года было несколько подобных инцидентов, самый известный из них привел к практически глобальной недоступности сервиса YouTube в 2008 году. Однако, начиная с 2013 года использование данной конструктивной уязвимости BGP встало на поток, а задачи, решаемые атакующими, стали шире. Теперь это не только атаки на отказ в обслуживании, но и перехват трафика (man-in-the-middle), а также использование чужого адресного пространства для других видов хакерской деятельности: рассылка спама, обычные DoS атаки итд. На круглом столе NANOG коллеги из Cisco Systems и BGPMon.net подтвердили наблюдения **Qrator Labs**.

При отсутствии методов непосредственной борьбы с BGP Hijacking единственным решением остается внешний мониторинг, который может позволить оперативно реагировать на возникающие проблемы в глобальной маршрутизации. Для реализации данной амбициозной задачи компания **Qrator Labs** запустила проект radar.qrator.net, который предоставляет разнообразную аналитику на междоменном сетевом уровне, в том числе, данные по циклам маршрутизации и обнаруженным ботнетам. В ближайшее время **Qrator Labs** также сможет предоставлять информацию об аномальных маршрутах в сообщениях протокола BGP, что позволит анализировать и пресекать инциденты с неавторизованным перенаправлением трафика.

О компании Qrator Labs

Qrator Labs (в прошлом HighloadLab) основана в 2009 году. Компания предоставляет услуги противодействия DDoS-атакам и является признанным экспертом в этой области. В 2010 году компания запустила сеть фильтрации трафика **Qrator** как технологическую основу коммерческого сервиса для защиты сайтов от подобных угроз. Алгоритмы и технологии, которые используются для противодействия атакам на сайты клиентов, являются know-how компании. Команда **Qrator Labs** занимается исследовательской деятельностью в области защиты от DDoS, начиная с 2006 года, и постоянно совершенствует алгоритмы, технологии и приемы противодействия DDoS-атакам.

Первыми клиентами **Qrator Labs** стали web-сервисы, испытывающие высокие нагрузки, – портал Хабрахабр и рекламная сеть Блогун. На сегодняшний день сервисом пользуются многие крупные компании из различных отраслей, такие как ведущие СМИ (газета «Ведомости», радиостанция «Эхо Москвы», газета «Известия», телеканалы «Дождь», ТНТ-Телесеть), банки (банк «Тинькофф Кредитные Системы», Связной Банк, ЮниКредит Банк, Сбербанк Украина), сайты электронной коммерции (Lamoda, Юлмарт, Enter, Эльдорадо, Groupon, Biglion) и другие.

Контакты для прессы

Иван Мирошниченко

PR&Marketing Qrator Labs
office: 8-800-3333-LAB (522)
skype: ihvans
mob: 8 916 925 29 47
im@highloadlab.com