DDoS-GUARD: когда мировая слава не в радость

До недавнего времени не слишком известная на международной арене российская компания DDoS-GUARD, специализирующаяся на защите от DDoS-атак и доставке контента, в начале 2021 года внезапно прославилась на весь мир, благодаря одному из своих клиентов - попавшей в опалу соцсети Parler, популярной у сторонников теперь уже бывшего президента США Дональда Трампа.

Информацию о том, что заблокированная Parler смогла частично восстановить свою работу с помощью российской компании, 19 января распространило агентство Рейтер со ссылкой на эксперта по IT-инфраструктуре Рональда Гилметта (Ronald Guilmette), который заметил, что новый IP-адрес Parler принадлежит DDoS-GUARD.

Вслед за Рейтер новость подхватили и другие издания. Но внимание зарубежной прессы к DDoS-GUARD оказалось специфическим: ростовского провайдера заподозрили и в пособничестве трампистам, которые в ходе акций протеста в начале января ворвались в здание Капитолия и вступили в стычки с полицией; и в сотрудничестве с фишинговыми и связанными с киберпреступностью сайтами; и в поддержке ресурсов, продвигающих идеи расистского и правого толка, а также теории заговора, вроде QAnon. Ну и куда же без связей с властями: конечно DDoS-GUARD не преминули упрекнуть за то, что она якобы сливает данные клиентов российским госструктурам.

Перед тем, как углубляться в тему, приведем немного официальных данных о DDoS-GUARD или ООО ″ДДОС-ГВАРД″, как она зовётся в России. Компания основана в 2011 году Евгением Марченко и Дмитрием Сабитовым. Головной офис фирмы находится в Ростове-на-Дону. DDoS-GUARD предоставляет услуги фильтрации трафика для защиты от DDoS-атак розничным и корпоративным клиентам на базе собственной сети фильтрующих узлов, расположенных в Нидерландах, России, Казахстане, Китае и США. Также компания выступает в качестве провайдера услуг защищенного хостинга.

По данным RIPE, DDoS-GUARD входит в топ-15 провайдеров связи в России и занимает первое место среди специализированных сервисов защиты от информационных атак.

По поводу последних событий в DDoS-GUARD заявляют, что Parler действительно числится их клиентом, но отрицают, что предоставляют хостинг популярной у сторонников Трампа соцсети.

> "Компания DDoS-GUARD является провайдером сетевой безопасности, решения и продукты которого направлены в том числе на предоставление защиты сайтов от DDoS-атак. DDoS-GUARD не предоставляет услуги хостинга ресурсу Parler.com. И не вправе сообщать, какие именно услуги предоставляются клиентам в независимости от их направленности или аудитории - это противоречит политике конфиденциальности компании и законодательству", - сказано в комментарии, предоставленном пресс-службой.

Также в сообщении отмечается, что Parler не нарушает правила использования DDoS-GUARD и действующее законодательство США, поэтому компания не намерена препятствовать оказанию услуг клиентам, пока те не нарушают нормы права стран, в которых юридически находятся.

> ″При получении решения суда или другого компетентного органа на ограничение действий той или иной организации, мы действуем в соответствии с законодательством и политикой использования″, - подчеркнули в DDoS-GUARD.

Ростовский провайдер заверяет, что соблюдает законодательство стран, в которых предоставляет услуги клиентам, и не поддерживает радикальные организации, экстремизм, терроризм и незаконную деятельность. Компания также не придерживается какого-либо политического движения. Единственная политика, которая близка DDoS-GUARD - политика сетевого нейтралитета.

На своей странице в Facebook компания разместила отдельное сообщение, в котором опровергает обвинения в передаче данных российским госструктурам.

> ″Это совершенно не так. Во-первых, политика конфиденциальности не позволяет нам передавать данные клиентов. Во-вторых, мы не храним никакую информацию о клиенте помимо личных данных, которые клиент вносит при регистрации на нашем сайте. В том числе это могут быть неактуальные данные. Например, вымышленное имя или номер телефона.
>
> Действительно, несколько лет назад у нас был контракт на оказание услуг министерству обороны РФ. Но этот клиент являлся для нас таким же рядовым как и остальные. Никаких дополнительных услуг этому клиенту не было оказано″, - говорится тексте.

По запросу Nag.Ru в ростовской компании также поделились предысторией скандала в США, в центре которого DDoS-GUARD оказалась.

Все началось еще в ноябре 2020 года, когда на официальную почту DDoS-GUARD поступило письмо от партнера DDoS-GUARD - крупной сети дата-центров CoreSite в Лос-Анджелесе, на мощностях которой компания в 2019 году открыла узел фильтрации. Представитель CoreSite сообщил, что у DDoS-GUARD обслуживается запрещенная в США организация ″Хамас″, и компании необходимо срочно прекратить сотрудничество с ней, поскольку в противном случае дата-центру может грозить уголовная ответственность и многомиллионные штрафы.

В DDoS-GUARD пошли на встречу CoreSite и прекратили предоставление услуг связанному с ″Хамас″ клиенту, несмотря на действующую в США статью 230 закона об этике в сфере коммуникаций. Согласно ей, ″ни один поставщик или пользователь интерактивной компьютерной услуги не должен рассматриваться в качестве издателя или носителя любой информации, предоставленной другим поставщиком информационного контента″.

На этом в DDoS-GUARD посчитали инцидент исчерпанным, но утром 7 января 2021 года на их электронную почту снова пришло письмо от CoreSite. В нем говорилось, что с 8 января питание для арендованной DDoS-GUARD стойки будет отключено, а оборудование демонтировано. При этом американцы обвинили своих российских партнеров в обслуживании других сайтов, близких к организации ″Хамас″. В попытке урегулировать ситуацию DDoS-GUARD отправила 6 писем с объяснениями, но ни на одно из них так и не получила ответ. В итоге компании пришлось закрыть узел фильтрации трафика в Лос-Анджелесе.

Спустя пару дней в компании начали понимать, почему в CoreSite не пошли на диалог, когда обнаружили в Сети статью известного американского исследователя киберпреступлений Брайана Кребса. В своем материале, опубликованном на сайте Krebsonsecurity, кибер-аналитик компрометирует DDoS-GUARD и называет ее ″изворотливой российской фирмой″, которая предоставляет услуги не только террористической группировке ″Хамас″, но и сайту сторонников конспирологической теории QAnon и скандальному имиджборду 8chan, на котором активно обсуждался захват Капитолия сторонниками Трампа.

В DDoS-GUARD видят за этой публикацией политические мотивы и стремление найти пресловутый ″русский след″.

> ″Мы не отслеживаем политические последствия американских скандалов, все-таки мы гораздо больше озабочены технологиями и надежностью наших услуг. Вероятно, что волны от масштабных событий, происходящих в Вашингтоне будут распространяться в Интернете достаточно долго, и многие компании так или иначе ощутят на себе последствия изменения информационных ландшафтов″, - заявил гендиректор и основатель DDoS-GUARD Евгений Марченко в комментарии ″Эксперту Юг″.

Несмотря на нынешние трудности, DDoS-GUARD намерена остаться в США и собирается открыть узел фильтрации на восточном побережье Северной Америки, чтобы в полной мере обслуживать клиентов из стран Нового Света.

В своих пресс-релизах DDoS-GUARD неоднократно подчеркивает, что придерживается позиции сетевого нейтралитета, и что ни один провайдер не несет ответственность за контент клиента.

> ″Оператор связи или хостинг провайдер не обязан отслеживать и нести ответственность за размещаемый его клиентами контент – на этом принципе строится интернет. На нашем месте мог оказаться совершенно любой провайдер, размещенный на базе CoreSite, через сеть которого (возможно, даже без его ведома) начал идти трафик "нежелательных" сайтов″, - указывают в компании.

В DDoS-GUARD отметили, что в Соединенных Штатах есть официальный список террористических и запрещенных организаций, но названий 8chan и Qanon в нем нет, плюс, отсутствует перечень доменов, поддоменов и дочерних сайтов, которые подлежат блокировке или запрету на территории страны.

Кроме того, клиенты нередко переделывают сайты и их содержимое: изначально под защиту может встать онлайн-магазин мягких игрушек, а через месяц он уже продает алкоголь.

> ″Подобные изменения очень сложно отслеживать, особенно когда у вас сотни тысяч клиентов. Да, мы постоянно совершенствуем алгоритмы исследований и машинного обучения, но даже они не могут моментально определить связь между данными клиентов из наших баз и наполнением их электронных ресурсов или доменными именами″, - объясняют в DDoS-GUARD.

В компании называют сложившуюся ситуацию абсурдной.

> ″Мы не про политику. Мы – про защиту сайтов и про безопасный интернет. Мы не хотим делать выводы относительно предвзятого отношения к российской компании, однако, мы не можем игнорировать тот факт, что русский бизнес в Америке дискредитируют. Например, CoreSite попросил нас покинуть дата-центр якобы из-за поддержки организации X., которую мы исключили еще в ноябре 2020-го. Но при этом наши коллеги из Sucuri (дочерняя компания американской GoDaddy) с ноября 2020 года предоставляют услуги той же организации X. с тех пор, как мы перестали с ними сотрудничать. Но Брайан Кребс не упустил возможность сказать о том, что именно РОССИЙСКАЯ ″изворотливая″ компания нарушает баланс и стабильность демократического строя США″.