Раскрыты детали изощренной хакерской атаки на ресурсы ЕГЭ

Едва успев начаться, кампания ЕГЭ-2019 оказалась под прицелом хакеров. Да еще под каким! 31 мая и 1 июня прошли массированные DDoS-атаки на интернет-ресурсы Рособрнадзора, по оценке специалистов, качественно отличающиеся от предшествующих. О том, как это было, «МК» из первых рук узнал в Федеральном центре тестирования. Тем временем эксперты поделились своими версиями о глубинных причинах, стоящих за внешней стороной дела. На выходных стало известно: в течение двух дней хакеры атаковали интернет-ресурсы Рособрнадзора, стремясь нарушить работу сайта при помощи DDoS-атак — непрестанной отправки огромного количества запросов, своей массой блокирующих доступ к этим ресурсам и тем самым препятствующих их работе в штатном режиме.

31 мая была зафиксирована DDoS-атака, целью которой стали информационные ресурсы ФИПИ, а 1 июня прошла более массированная атака - на автоматизированные сервисы ЕГЭ, - рассказал «МК» о деталях замдиректора Федерального центра тестирования Станислав Афанасьев. - Атаки начались около 06.30 утра и продолжались около 4 часов.

Правда, хакерские атаки на ЕГЭ случались и раньше. Однако нынешняя вышла особой: «Мощность атаки составила более 6 Гбит в секунду. При этом если предыдущие хакерские атаки были в основном связаны с видеонаблюдением и порталом «Смотри ЕГЭ», то нынешняя была более точечной и нацеливалась сервисы Федерального института педагогических измерений и Федерального центра тестирования»,- уточнил Афанасьев.

Примечательно, что злоумышленники, по его словам, «подошли к делу изобретательно и искали уязвимые места в нашей обороне, а задействованные ими ресурсы были достаточно значимыми. Мы четко понимаем, что это была распределенная атака: было задействовано много ресурсов по всему миру как в России, так и за рубежом. Организаторы подготовились основательно: сетевые адреса, задействованные ими, чтобы осуществить акцию, надо было получить в свое распоряжение — арендовать или уже иметь. Таким образом, ресурсы, что называется, были ими подтянуты».

Впрочем, атаку, по его словам, «мы смогли отбить: остановок в работе значимых ресурсов не было, и атака не повлияла на обработку результатов прошедшего единого государственного экзамена».

В целом же «есть несколько методов борьбы с DDoS-атаками, и многие из них мы применяем. Что касается последней атаки, то для нас она стала сигналом. Мы мобилизовали как стандартные методики борьбы с атаками, так и задействовали альтернативные возможности. Если будет массированная атака, мы обеспечим непрерывность всех процессов и каналов доведения информации».

Эксперты-технари с предположением чиновника, что за последней DDoS-атакой стоят не психи или хулиганы-одиночки, а организованные силы, полностью согласны:

- В одиночку такую акцию не провести,- заверил «МК» специалист-айтишник Роман Перфилов. - 6 Гбит в секунду — это очень быстро! Для такой скорости нужно, чтобы человек сидел на магистрали трафика или, на профессиональном сленге - «на стволе». Все, что быстрее 1 Гбит — это точно группа! Люди явно написали программу, и с разных точек стали подавать запросы на сервер, выбранный как мишень для атаки.

Обычно это делается, когда хотят «завалить» какой-то сайт или структуру — как правило, государственную. Цель — вывести их на какое-то время из рабочего состояния. Ну а мотивы могут быть самыми разными — от чисто хулиганских до сугубо корыстных. Вопрос денег тут очень даже возможен!

В попытке докопаться до причин регулярных — и все ужесточающихся — нападок хакеров на ресурсы и сервисы ЕГЭ вопрос денег, действительно, приходит на ум одним из первых. Каждый год Рособрнадзор загодя предупреждает участников экзаменов: не покупайте якобы «верных» заданий ЕГЭ! Не ведитесь на якобы «верные» интернет-утечки! А ведь это — рынок, притом немалый. И потери в заработках вполне могли спровоцировать его участников на поощрение хакеров, пытающихся «сломать» ЕГЭ.

Можно предположить и другие способы нелегально нажиться на временном выводе из строя официальных сервисов ЕГЭ — например, «толкнуть» на пару дней раньше результаты экзаменов. И все они тоже в выигрыше.

- Мы очень мало знаем про «серую», хакерскую зону интернета. Так что там может быть все, что угодно,- заявила «МК» директор Центра экономики непрерывного образования Академии народного хозяйства и государственной службы при президенте России Татьяна Клячко.- Если хакерам пообещали значительные деньги за то, чтобы в интересах нелегального ранка «положить» ресурсы ЕГЭ, они легко могут это сделать. Для них вопрос не в том, ЕГЭ это или не ЕГЭ, а в том, чтобы им заплатили определенную сумму.

Кстати, столь же охотно, по мнению Клячко, те же хакеры подрядятся «завалить» ЕГЭ, если им заплатят оппоненты этой процедуры: «Недовольство едиными госэкзаменами в обществе по-прежнему есть, - подчеркнула она.- Так что желание дискредитировать этот инструмент также не стоит сбрасывать со счетов».

Наконец, не стоит исключать и желание дискредитировать государство или как минимум орган государственной власти в лице Минпросвета с Рособрнадзором.

- Я не исключаю, что это был удар по престижу государства, стремление показать его слабость,- поделился с «МК» депутат Государственной Думы Михаил Берулава. - Уж больно серьезной оказалась атака!

Действительно, при всех продолжающихся у нас спорах о ЕГЭ, несомненны две момента. Во-первых, данная модель итоговых испытаний прочно заняла свое место в системе образования нашей страны. Во-вторых, ее многолетнее усовершенствование сделало ее максимально открытой и прозрачной. Ведь как ни относись к единым госэкзаменам как таковым, а исключение человеческого фактора из доставки в оба конца экзаменационных материалов или, скажем, открытая публикация результатов практически свели на нет риск злоупотреблений, еще недавно процветавших на ниве выпускных и вступительных экзаменов. Ну а это крушит рынок «черных» и «серых» околообразовательных услуг. И тому это, понятно, не в радость.