Судьба одного хакера

В августе 2017 года хакерское сообщество облетела новость: в Лас-Вегасе ФБР задержало Маркуса Хатчинса (Marcus Hutchins), того самого, что тремя месяцами ранее остановил эпидемию вируса-шифровальщика WannaCry, убыток от которой по всему миру эксперты оценили в 1 миллиард долларов. Потери могли быть куда серьезнее, если бы не 23-летний специалист по кибербезопасности из Британии, который практически случайно нашел способ не допустить дальнейшего распространение вирусной атаки.

Однако Хатчинс недолго наслаждался обрушившейся на него славой: в Америке, куда он приехал на хакерскую конференцию DefCon, недавнего героя обвинили в киберпреступлениях и арестовали. Молодой человек до сих пор дожидается суда в США и не может вернуться на родину. О перипетиях в судьбе хакера, имя которого прогремело на весь мир в прошлом мае, рассказывает американский журнал New York Magazine.



Остановив WannaCry, Хатчинс превратился в настоящую знаменитость: его лично поздравил экс-агент АНБ Эдвард Сноуден, статьи о нем опубликовали ведущие издания, а Cisco пригласила на крупнейшую хакерскую конференцию DefCon в качестве VIP-участника. За год до этого Маркус побывал на мероприятии, но оно оставило не самые приятные впечатления.

> "Помню, как я медленно двигался в толчее по холлу, заполненному морем людей, от которых разило так, будто они не мылись несколько дней", - вспоминает он.

Но на DefCon 2017 все было совсем по-другому: Хатчинс стал звездой, с которой каждый норовил сфотографироваться, а потом выложить снимок онлайн с хэштегом #WannaCrySlayer (#убийца WannaCry).



В Лас-Вегас Хатчинс устроил себе отдых, о каком только может мечтать 23-летний парень: снял через

сервис Airbnb апартаменты с самым большим частным бассейном, побывал на стрелковом полигоне, где палил из пулемета, разъезжал по городу на арендованном Lamborghini, бродил по казино, но не для того, чтобы играть, а ради бесплатной выпивки. Словом, Хатчинс так увлекся, что не заметил за собой слежки американских спецслужб. Когда в аэропорту, где Маркус дожидался своего рейса, чтобы лететь домой, к нему подошли несколько агентов и попросили пройти с ними, это стало для молодого человека полной неожиданностью.

Хатчинс не знал, что еще до въезда в США окружной суд штата Висконсин обвинил его в причастности к созданию и распространению банковского трояна Kronos. За подобные преступления в Америке может грозить до 40 лет тюрьмы.

Проведя под арестом выходные, Маркус предстал перед судом в Милуоки, где он заявил о своей невиновности. Хатчинса выпустили под залог в 30 тысяч долларов. Сумму за него внес сочувствующий хакер, с которым британец никогда не встречался.



Маркусу запретили покидать страну, и в ожидании следующих судебных заседаний "убийце WannaCry" пришлось осесть в Лос-Анджелесе, где расположен офис ИБ-компании Kryptos Logic, на которую он работает.

Постепенно американская Фемида смягчила ограничения (сначала Хатчинса посадили под домашний арест, затем перевели на комендантский час и обязали носить GPS-маячок на щиколотке), но прежняя жизнь юноши была практически разрушена. Маркуса бросила девушка, а на новые отношения в его положении вряд ли стоило рассчитывать. Хотя адвокаты защищали Хатчинса на безвозмездной основе, большую часть своих сбережений в биткоинах ему пришлось продать, чтобы оплатить консультации с юристами по иммиграционным вопросам и налогообложению. Маркус плохо спал и не мог работать (одним из условий его освобождения под залог был запрет пользоваться интернетом, который позднее сняли, так же, как и GPS-браслет).

> "ФБР отняло у меня все: работу, девушку, биткоины", - пожаловался Хатчинс в интервью журналисту New York Magazine Ривзу Уидеману, которое состоялось в феврале 2018 года в курортном городке Санта-Моника на западе Лос-Анджелеса.

Часть заметки о победителе WannaCry посвящена экскурсу в его биографию. Маркус вырос в городе Илфракомб на юго-западном побережье Англии, где живет около 11 тысяч человек. Начав осваивать программирование с 12 лет, к старшим классам он уже настолько в этом поднаторел, что школьная администрация заподозрила его в кибератаке, которая вывела из строя серверы учебного заведения. Впрочем, сам Хатчинс настаивает на своей невиновности.

После окончания школы он два года проучился в местном техникуме, где уровень преподавания информатики казался ему слишком примитивным. В 2013 году Маркус начал вести блог Malwaretech.com, где делился своими любительскими открытиями в области так называемого обратного проектирования (англ. reverse engineering) - одного из ключевых направлений сферы информационной безопасности, суть которого заключается в анализе вредоносного ПО для раскрытия механизмов его работы. В одной из статей под заголовком "Вирусы шутки ради, а не для наживы (ведь последнее противозаконно)" Хатчинс посетовал на отсутствие достойных объектов для анализа и признался, что из-за этого сам попробовал написать вредоносную программу. Впрочем, он тут же успокоил читателей блога: созданный им буткит для Windows XP существует только в экспериментальной версии, которую нельзя использовать для атаки.

Хотя Хатчинс пытался найти работу в ИБ-сфере и даже подавал заявку в Центр правительственной связи Великобритании (Government Communications Headquaters, GCHQ) - аналог Агентства

национальной безопасности в США, он утверждает, что увлекся хакерством от нечего делать и никогда не планировал строить на этом карьеру.

Как бы там ни было, в 2015 году молодого человека заметил гендиректор ИБ-компании Kryptos Logic Салим Неино, который прочел заметку Хатчинса о бот-сети Kelihos и сразу же предложил ему работу.

> "Он очень одарен. Определенным вещам можно научить, но в сфере компьютерной безопасности крайне важно иметь задатки от природы", - охарактеризовал британца его американский начальник.

И вот, в 22 года Хатчинс вдруг стал получать зарплату из шести цифр, при этом имея в подчинении двух людей и работая дистанционно по удобному ему графику из своей спальни в родном доме. Он быстро заработал репутацию в мире ИБ-профессионалов, нередко бескорыстно помогая коллегам. В 2017 году Хатчинса пригласили к участию в инициативе Национального центра кибербезопасности Великобритании по привлечению к работе на правительство самых лучших и талантливых ИБ-экспертов страны.

Когда в мае 2017 года Хатчинс впервые услышал о вирусе-вымогателе WannaCry, то не придал новостям особого значения, поскольку подобные инциденты уже успели стать привычными. Однако атака, для которой хакеры задействовали эксплойт EternalBlue, использующий уязвимость сетевого протокола Windows SMB, продолжала набирать обороты, и Хатчинс заинтересовался.

Раздобыв образец WannaCry у одного из своих друзей, британец разобрал вредонос "по косточкам". Анализ программного кода показал, что вирус запрашивает несуществующий домен iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, что натолкнуло на идею зарегистрировать такое имя. Сделав это, Хатчинс остановил дальнейшее распространение вируса, которое запускалось в случае неуспешного запроса домена.

Через пару дней СМИ выяснили, кто стоит за спасением мира от WannaCry, и фотографии Маркуса запестрили на обложках таблоидов. Хатчинса осаждали репортеры, интервью с ним опубликовало одно из крупнейших новостных агентств Associated Press, а число подписчиков его аккаунта в Twitter увеличилось вчетверо.

В киберсообществе заслуги британца и вовсе превозносили до небес. Маркусу вручили почетную награду SC Awards Europe, которая свидетельствует о высшем признании в сфере информационной безопасности.

Однако триумф Хатчинса был непродолжительным: он закончился вместе с конференцией DefCon и шикарным отпуском в Вегасе, когда в аэропорту его задержали агенты ФБР. Британца подозревают не только в создании вредоносного ПО Kronos, воровавшего с компьютеров вводимые данные для платежей, но и в сговоре с целью продажи вируса киберпреступникам и рекламе троянца на подпольной онлайн-площадке AlphaBay, закрытой в результате масштабной международной операции в июле 2017 года.

Среди ИБ-профессионалов новость восприняли как гром среди ясного неба. В кои-то веки хакер стал героем, и вдруг такой конфуз - он, оказывается, киберпреступник. На Хатчинса внезапно посыпались нападки и голословные обвинения, мол, это он и создал WannaCry, а остановил атаку только потому, что та вышла из-под его контроля. Но версия не нашла подтверждения: власти США и других стран возложили ответственность за WannaCry на северокорейских хакеров из группировки Lazarus.

Некоторые ударились в конспирологию и говорили, что все обвинения сфабрикованы с целью заставить Хатчинса быть сговорчивее со спецслужбами и теснее с ними работать. Хатчинс неоднократно сотрудничал с правоохранительными органами, в том числе и в деле с WannaCry. Он даже публично благодарил ФБР за помощь.

Другие, стремясь защитить британца, утверждали, что ему не хватило бы опыта для создания Kronos. Такое "оправдание" вызывает у Хатчинса не меньшую досаду, чем необоснованные нападки.

> "Даже не знаю, что обиднее: когда тебя считают негодяем, или когда ставят под сомнение твои способности программиста", - признался молодой человек.

Между тем, месяц спустя после ареста Хатчинса журналист Брайан Кребс, освещающий тему кибербезопасности, в своей статье рассказал о выявленной им связи между личностью британца и несколькими хакерскими никами, замешанными в незначительных киберпреступлениях, которые были совершены в бытность Хатчинса подростком. Хотя журналист не нашел свидетельств того, что Маркус имеет отношение к созданию Kronos, после публикации пошли разговоры, что прошлое юноши далеко небезупречно.

Впрочем, темные страницы в жизни Маркуса ничуть не смущают его начальника, Салима Неино.

> "Как же еще таким людям, как Маркус, оттачивать свой талант? Чтобы совершенствоваться,

ИБ-специалистам нужно сталкиваться с реальными угрозами. Поэтому многие из них посещают теневые хакерские форумы и водят дружбу с киберпреступниками", - отмечает глава Kryptos Logic.

В киберсообществе сплошь и рядом встречаются те, кто с темной стороны перешел на светлую. Подростками многие из них испытывали границы дозволенного и преступали закон, говорит Кейти Муссурис (Katie Moussouris), известная личности среди хакеров, которая теперь стала официальным представителем платформы HackerOne, организующей конкурсы поиска уязвимостей. По ее словам, в юности нередко хочется пуститься во все тяжкие, доказать свою значимость и мастерство, получить признание.

Даже прокуроры, выдвинувшие обвинения против Хатчинса, признают, что его предполагаемые преступления - "дела давно минувших дней" и не считают британца общественно опасным. Иначе, почему с него сняли все ограничения на доступ в интернет - крайне необычная практика в подобных случаях.



По данным правоохранителей, на допросе сразу после ареста в аэропорту Лас-Вегаса Хатчинс признался в создании Kronos, однако адвокаты утверждают, что агенты ФБР надавили на юношу, плюс, во время дачи показаний он страдал от недосыпания и был пьян. Также американские власти располагают распечаткой онлайн-чатов Хатчинса, в которых он якобы общался с другим неустановленным подозреваемым по поводу продажи Kronos и дележа полученной прибыли.

Хатчинс не отрицает, что в прошлом он мог совершать сомнительные поступки, однако в деле о Kronos он отказался от данных под давлением показаний и теперь настаивает на своей невиновности. Обсуждать с журналистом детали Маркус не стал, сославшись на то, что судебное разбирательство еще продолжается.

Впрочем, Хатчинс и так наказан: юноша опасается, что даже если дело получится уладить, его репутации уже нанесен непоправимый ущерб. В бизнесе по обеспечению кибербезопасности все строится на доверии, и после выдвинутых против него обвинений Маркус боится остаться без работы.