Кто хочет стать миллионером? Шесть хакеров заработали $1 млн с помощью HackerOne

Платформа HackerOne, объединяющая "белых" или этичных хакеров, которые помогают компаниям выявлять и устранять уязвимости в киберзащите, пополнила свой список миллионеров. Теперь в нем шесть человек : все они официально заработали больше миллиона долларов, участвуя в организованных HackerOne мероприятиях Bug Bounty, в которых профессионалы в области информационной безопасности (ИБ) за деньги находят слабые места в программном обеспечении и бреши в киберзащите компаний.

Журнал Forbes рассказал о хакерах-миллионерах, преуспевших с помощью HackerOne, и узнал о других последних достижениях платформы.



К августу 2019 года услугами сервиса пользуются более 1500 организаций, включая такие крупные, как General Motors, Goldman Sachs, Google, Intel, Microsoft, Nintendo, Lufthansa, Spotify, Starbucks и Twitter. К помощи хакеров, зарегистрированных в HackerOne, прибегают даже государственные ведомства, в том числе Министерство обороны США.

> "У HackerOne уже почти полмиллиона зарегистрированных хакеров, и каждый день к сервису присоединяются 600 новых участников. На сегодняшний день они сумели обнаружить в общей сложности более 130 тысяч уязвимостей", - говорит ИБ-инженер HackerOne Лори Мерсер (Laurie Mercer).

Идея выплачивать вознаграждения за найденные уязвимости, конечно, не нова. Мерсер считает, что впервые поиск багов за деньги опробовали еще 30 лет назад, когда любому нашедшему дефект в операционной системе, управляющей космическим телескопом "Хаббл", пообещали награду в 1000 долларов.

С тех пор схема Bug Bounty успела получить широкое распространение. HackerOne, ведущая ИБ-платформа, привлекающая к поиску уязвимостей хакеров из более чем 150 стран мира, за время своей работы выплатила вознаграждений на общую сумму почти в 65 миллионов долларов. По словам Мерсера, самая внушительная награда, полученная одним баг-хантером в рамках HackerOne, на сегодняшний день составляет 100 тысяч долларов. Это в 200 раз больше суммы первого вознаграждения, который сервис HackerOne выплатил хакеру еще в 2013 году.



Только за последний год участники Bug Bounty-программ HackerOne заработали 21 миллион долларов, улучшив предыдущий годовой результат на 10 миллионов долларов. Ведущие корпорации, такие как Google, Microsoft, Apple и Intel, за выявление критических уязвимостей предлагают индивидуальные премии на сумму до 1,5 миллиона долларов.

Средний размер вознаграждений за серьезные уязвимости, конечно, гораздо меньше, но тоже впечатляет. За последний год сумма выросла почти на 50% и составила 3384 доллара против 2281 доллара в 2017-м и 1977 долларов в 2016 годах.

Гендиректор HackerOne Мартен Микос (Marten Mickos) прогнозирует, что к завершению 2020 года участники платформы доведут свой совокупный заработок до 100 миллионов долларов. Также ожидается. что этому времени число этичных хакеров, зарегистрированных в HackerOne, достигнет 1 миллиона.

То, насколько прибыльной может быть карьера хакера, своим примером недавно продемонстрировали участники Black Hat и DEF CON. Эти крупнейшие хакерские конференции традиционно проводятся в американском Лас-Вегасе в августе. Неделю, в течение которой проходят мероприятия, в шутку прозвали летним хакерским лагерем (Hacker Summer Camp).



На хакатоне H1-702, организованном в рамках конференций, около 100 баг-хантеров сообща охотились за уязвимостями. В общей сложности они нашли более 1000 ошибок, а совместный заработок, который хакеры разделили между собой, превысил 1,9 миллиона долларов.

Среди участников хакатона были и новоиспеченные миллионеры HackerOne. Кто же они?

Первый из них - 19-летний **Сантьяго Лопес (Santiago Lopez) из Аргентины** , который открыл список

миллионеров в марте 2019 года.



Молодой человек, известный в киберсообществе под псевдонимом try_to_hack, присоединился к HackerOne в 2015 году. За время участия в проекте Сантьяго Лопес выявил более 1676 уязвимостей, в том числе для таких клиентов, как Twitter, Verizon и правительственные организации США.

Как признается юноша, он - 100-процентный хакер-самоучка, и все, что знает, почерпнул в интернете, просматривая обучающие видео и читая книги. Поначалу юный хакер не представлял, какие деньги может зарабатывать. Первая награда Сантьяго, которую он получил в 2016-м в возрасте 16 лет, составляла 50 долларов.

> "На поиск первой уязвимости у меня ушло много времени. Потребовалось немало терпения и сил, но я добился своего, и оно того стоило", - вспоминает Сантьяго.
>
> "Я очень горжусь, что мою работу признают и ценят. И дело не только в деньгах. Мои достижения означают, что информация компаний и людей теперь более защищена, чем раньше, и это очень здорово", - сказал юноша в интервью для блога HackerOne.

Второй миллионер HackerOne - **Марк Личфилд (Mark Litchfield)**, работающий под ником mlitchfield. Родом из Британии, он намного старше Лопеса и считается в HackerOne ветераном ИБ-отрасли.



До того, как освоить свою нынешнюю профессию, Личфилд держал в Шотландии магазинчик по продаже компьютеров, но не преуспел в этом бизнесе. В 1999-м, по совету своего брата Дэвида, который уже работал в ИБ-сфере, Марк окончил курсы по Windows Server NT4, а затем отправился в Лондон. Там и началась его карьера специалиста по кибербизопасности.

Дэвид и Марк основали свою ИБ-фирму, специализирующуюся на поиске уязвимостей, а в 2000 году продали ее. Еще год спустя они создали другую компанию, которая через восемь лет вновь была куплена. В 2013-м Личфилд увлекся тестированием на проникновение, а затем стал участвовать в программах Bug Bounty, что позволило ему поправить свои финансы.

> "Путь к хакерству открыт для любого, у кого есть лэптоп и кто интересуется кибервзломами. Надеюсь, наши достижения вдохновят других хакеров, молодых и не очень, на то, чтобы попробовать свои силы и стать частью нашего сообщества, а заодно срубить баксов и повысить безопасность интернета для людей", - заявил Марк Личфилд.

Хакер-миллионер номер три - **Франс Розен (Frans Rosén) из Швеции.** Участник HackerOne с 2013 года (fransrosen), он не только один из самых известных баг-хантеров платформы, но еще и предприниматель, имеющий свой успешный ИБ-бизнес. Портал Hackread поставил Франса Розена на второе место в своем рейтинге "Топ-10 самых знаменитых баг-хантеров всех времен". Результаты его исследований в области безопасности освещались многими международными изданиями, такими как Observer, BBC, Ars Technica и SC Magazine.



Продолжает список 24-летний **австралиец Натаниэль Уэйклэм (Nathaniel Wakelam).** В HackerOne он с 2013 года под именем nnwakelam, но также известен под ником Naffy. Молодой человек никогда не проводит в одном месте больше месяца, но сейчас страной базирования выбрал Таиланд.



Обнаружив первый баг еще учеником начальной школы, Натаниэль с тех пор добавил в свою "копилку трофеев " еще более 700 уязвимостей. С учетом этого Уэйклэм считается одним из самых результативных участников сервиса HackerOne. В свободное от хакерства, путешествий и развлечений время он участвует в благотворительном проекте "Hackers Helping Hackers", который помогает молодым хакерам начинать карьеру баг-хантера. Еще одно "детище" Уэйклэма - компания Gravity, работающая в сфере ИБ-консалтинга, где молодой человек занимает пост директора по информационной безопасности.

> "Проекты Bug Bounty дали мне такие возможности, о которых я не мог и подумать. Когда я начинал, лишь немногие компании привлекали хакеров к поиску уязвимостей, отрасль только зарождалась. Шесть лет спустя ситуация резко изменилась. Благодаря Bug Bounty я могу работать из любой точки мира, общаться с уважаемыми мной профессионалами, получать дополнительный доход и развивать другие бизнес-начинания. Я рад, что вместе с

коллегами одним из первых достиг знакового рубежа [в $1 млн]) и призываю всех, кто хочет добиться такого же результата - просто сделайте первый шаг и начните, шансы есть, если вы готовы ими воспользоваться", - сказал Натаниэль Уэйклэм.

Среди миллионеров HackerOne также числится 35-летний **американец Томми ДеВосс (Tommy DeVoss), он же dawgyg.** В начале своего хакерского пути молодой человек встал на "темную сторону": в 2000-м его осудили за кражу учетных записей AOL с целью проникновения в компьютерные системы военных. На счету Томми было уже два тюремных срока, и третий грозил стал пожизненным, когда он резко изменил свою жизнь. Сначала молодой человек устроился на нормальную работу в ИТ-сфере, а позднее познакомился и с HackerOne. С 2014 года он не по наслышке знает, что на хакерстве можно хорошо зарабатывать и не нарушать при этом никаких законов. Только за трехдневный хакатон H1-702 Томми ДеВосс получил вознаграждения на сумму 130 тысяч долларов.



Замыкает шестерку 28-летний **Рон Чен (Ron Chan) из Гонконга** (ngalog). Как и другие участники HackerOne, Чен увлечен поиском брешей в киберзащите технологических гигантов. Среди компаний, вознаградивших юношу за последнее время - Airbnb, GitLab, PayPal и Uber. Только в июле 2019 года Чен заработал в рамках HackerOne порядка 75 тысяч долларов. Неудивительно, что он попал в список миллионеров сервиса, хотя присоединился к платформе только в 2016 году.



Комментируя свое достижение, Чен отметил, что никогда не думал, что сможет стать одной из звезд платформы и на равных работать, общаться и состязаться с другими ведущими хакерами.

> "Эти шесть хакеров - прекрасный пример для любого, кто задумывается, как наилучшим образом извлечь выгоду из своих хакерских навыков. Участвуя в программах Bug Bounty, специалисты по кибербезопасности сегодня могут получать в 40 раз больше, чем в среднем зарабатывают инженеры-программисты. Это новая профессия, на которой хакеры могут получать щедрое вознаграждение за то, что, находя баг за багом, они помогают делать цифровой мир безопаснее", - подытожил ИБ-инженер HackerOne Лори Мерсер.

