Этичные хакеры: кибервзломы во благо

Этичные или "белые" хакеры (white-hat) зарабатывают тем, что взламывают компьютерные системы компаний, но не в криминальных целях, а чтобы проверить надежность киберзащиты и выявить в ней слабые места. Белые хакеры, в отличие от черных (black hat), не совершают преступлений. Многие из них официально работают на государство или на крупные корпорации в качестве специалистов по информационной безопасности (ИБ). Есть и те, кто практикуют хакерство, как хобби и развлечение.

Впрочем, далеко не все кибервзломы санкционированы руководством компаний. В свободное от работы время - вечерами и в выходные дни - ИБ-энтузиасты нередко участвуют в неофициальных, "побочных" проектах. Один из таких - недавний взлом системы управления "умным" домом Zipato, в результате которого "белые" хакеры Чарльз Дардаман (Charles Dardaman) и Джейсон Уилер (Jason Wheeler) выявили несколько серьезных уязвимостей в программном обеспечении разработчика.

На идею взломать смарт-замок друзей натолкнула коллега по ИБ-отрасли Лесли Кархарт (Lesley Carhart). Владелец дома, где она арендовала квартиру, начал устанавливать "умные" замки, из-за чего Лесли даже пришлось сменить место жительства. Дардаман и Уилер хотели показать своим экспериментом, что опасения по поводу надежности смарт-замков не лишены оснований.

У друзей ушел день на то, чтобы "хакнуть" смарт-замок Zipato на входной двери, но не это было их главной целью. Хакеры хотели добраться до смарт-хаба ZipaMicro - системы, используемой Zipato для управления устройствами "умного" дома. Через пару дней им удалось и это.

Проникнув в систему, Дардаман и Уилер обнаружили на карте памяти устройства SSH-ключ, дающий root-привелегии, который оказался одинаков для всех смарт-хабов ZipaMicro. Узнав SSH-ключ, хакеры получили доступ к зашифрованным паролям всех контроллеров и могли управлять любым "умным" домом, где имеются устройства Zipato.

Дардаман и Уилер сразу же связались с разработчиком и уведомили его о своих открытиях. В интервью изданию The Vox хакеры признались, что в компании не очень-то обрадовались вестям, но через несколько недель исправили допущенные ошибки.



Когда уязвимости были устранены, Дардаман обнародовал информацию в интернете, а также поделился отчетом об эксперименте со смарт-замком Zipato с журналистами TechCrunch. Новость быстро разлетелась по Сети и вызвала большой резонанс.

Надо сказать, эта и другие хакерские "проделки" приносят реальную пользу с точки зрения обеспечения безопасности пользователей.

Например, в 2015 году хакеры сумели перехватить управление Jeep Cherokee через уязвимости мультимедийной системы Uconnect, после чего производитель был вынужден отзывать 1,4 миллиона автомобилей для устранения ошибок в программном обеспечении.

В 2018 году хакеры из группировки Anonymous Calgary Hivemind подключались к камерам наблюдения Nest, чтобы продемонстрировать их уязвимость. В результате разработчик камер - принадлежащая Google компания Nest - инициировала сброс паролей и предложила пользователям перейти на двухфакторную аутентификацию.

В марте 2019-го много шума наделали новости о критической уязвимости в кардиодефибрилляторах компании Medtronic, позволяющей с помощью радиосигналов получить полный контроль над устройством с расстояния до 6 метров. В настоящее время Управление по контролю за продуктами и лекарствами США (The Food and Drug Administration) совместно с Medtronic работают над устранением проблемы, внимание на которую, опять-таки, обратили хакеры.

Несмотря на приведенные примеры, слово "хакер" в сознании большинства прочно ассоциируется с чем-то противозаконным. Этичные кибервзломщики считают это несправедливым.



> "Есть ведь такие понятия, как лайфхак (от англ. life hack - житейская хитрость, полезный совет) и трэвелхак (от англ.и travel hack - рекомендации для путешественников о том, как дешево или бесплатно совершать авиаперелеты, останавливаться в отелях, арендовать автомобили и т. п.), и у них нет негативной коннотации. Но как только "хакер" звучит в компьютерном контексте, тут же в воображении людей возникает пугающая темная фигура в капюшоне", - сетует хакер, известный в киберсреде под ником wirefall (свое настоящее имя попросил не называть).

Рассуждая о предвзятости, он с обидой заметил, что слесарей не донимают вопросами, отчего они не промышляют кражами со взломом.

Негатив со стороны компаний - тоже обычное дело. В то время как одни организации ценят труд этичных хакеров, другие воспринимают их скорее как врагов, и чуть ли не приравнивают к киберпреступникам. По мнению wirefall, причина враждебности в том, что многие фирмы просто не хотят заботиться о безопасности, поскольку им гораздо дешевле заплатить штраф, чем обеспечить киберзащиту на должном уровне.

Поскольку эффективное регулирование в данной сфере пока отсутствует, некоторые хакеры считают, что внимание СМИ и общественности - это лучший способ воздействовать на такие компании.

"Темная сторона" никогда не привлекала Чарльза Дардамана.

> "Я хотел жить нормальной жизнью. И заработать на пенсию", - признается 20-летний юноша журналистам The Vox.

Молодой человек живет в Далласе и в свободное от работы время увлекается компьютерными играми. Кстати, они-то и подтолкнули Дардамана к будущей профессии. Еще в старших классах школы он начал писать чит-коды для популярной игры Minecraft и увлекся программистскими головоломками, которые по роду своей работы решают легальные хакеры. Когда Дардаман окончил

университет со степенью в области информационных технологий, он уже знал, что будет этичным хакером.



Сегодня молодой человек работает на компанию Critical Start, которая на контрактной основе привлекает этичных хакеров для проверки киберзащиты крупных корпораций и банков. Critical Start и другие подобные ей фирмы - часть развивающейся индустрии информационной безопасности, призванной остановить растущую волну кибератак.

ИБ-отрасль начала расширяться в начале двухтысячных, на фоне первых утечек данных, появления социальных сетей и развития онлайн-торговли. В те времена "белыми" хакерами нередко становились пойманные властями киберпреступники. Теперь все изменилось: молодые люди, такие как Дардаман, могут еще в школе попробовать свои силы в этичном хакинге и получить онлайн-сертификат, подтверждающий квалификацию в сфере кибербезопасности.

Большинство контрактных проектов, в которых участвует Дардаман, длятся неделю или две. Нередко компания не предупреждает свою команду киберзащиты о предстоящей проверке, позволяя хакеру присмотреться к тому, как работают компьютерные сети и найти возможность для проникновения вглубь ИТ-систем. Но такая игра в кошки-мышки продолжается только несколько дней.

> "Моя цель - к концу недели громко заявить о себе, - рассказывает хакер, отмечая, что обычно он старается получить доступ к корпоративным серверам, заставляя отреагировать ИБ-команду.
> Если за неделю им не удается меня поймать, это значит, что компании следует пересмотреть меры кибербезопасности".



В свободное от работы время Дардаман практикует взломы устройств интернета вещей, чтобы показать людям, что они не до конца осознают все риски, которые несет с собой установка в доме различных "умных" гаджетов с датчиками, голосовым управлением и возможностью доступа к ним через интернет. По словам хакера, подобные кибератаки для него - как игра.

> "Лучший способ защитить ИТ-систему - это проверить ее эффективность с помощью противника, посмотреть, как ее попытаются взломать киберпреступники, хактивисты или разведслужбы", - убежден Филипп Уайли (Phillip Wylie), специалист по тестам на проникновение (pentest) в банке US Bank и профессор Ричландского колледжа по этичному хакингу.

Как и Чарльза Дардамана, Уайли привлекают в хакерстве возможность решать интеллектуальные головоломки и эмоциональный подъем от успешного проникновения в закрытую систему. До того, как устроиться в US Bank, Уайли работал консультантом и тестировал на устойчивость к взломам и кибератакам веб-приложения. Однажды он обнаружил у клиента серьезную уязвимость, позволившую проникнуть в корневую базу данных компании.

> "Я мог делать все что угодно: добавлять в систему новых пользователей, копировать базу данных, удалять записи или вовсе отключить сервер", - вспоминает специалист.

Некоторые хакеры не ищут уязвимости. Например, 23-летняя Джейн Маньчунь Вон (Jane Manchun Wong) из Гонконга с помощью реверс-инжиниринга приложений выясняет, что новенького для своих пользователей готовят разработчики.



> "Эта информация в смартфонах всех пользователей. Да, она глубоко спрятана, но ничего незаконного в ее раскрытии нет. Это публичная информация", - рассказывает Джейн Вон о своем увлечении.

В апреле 2019 года исследовательница рассказала, что разработчики Instagram хотят спрятать количество лайков под фотографиями, чтобы стимулировать блогеров создавать больше контента. Поначалу в соцсети отрицали подобные планы, но в мае Instagram перестал показывать счетчик лайков в Канаде, а в начале августа это же произошло с лентами пользователей в Австралии, Бразилии, Италии, Ирландии, Новой Зеландии и Японии.

Вместе с тем, как и этичные хакеры, Вон преследует благие цели. Например, если она обнаруживает в коде приложения пользовательские данные, то сообщает об этом компании, чтобы предотвратить возможную утечку. По словам Вон, она занимается этим для удовольствия - ей тоже нравится решать головоломки.

> "С тех пор, как моими открытиями заинтересовались, и компании начали следить за моими твитами, разработчики стали повышать безопасность своих приложений. Это одно из соображений, по которым я этим занимаюсь....Компании повысят защиту приложений, и взломать их будет сложнее", - пояснила Джейн Вон в интервью BBC.

Большинство "белых" хакеров заявляют, что они не пытаются выставлять компании в плохом свете. Обнаружив уязвимость, ИБ-специалисты оповещают организацию и дают ей время на исправление ошибки. Обычно срок составляет 90 дней в соответствии с правилами Google Project Zero.

> "Если они реагируют на предупреждение и устраняют уязвимость - отлично. Но если говорят, что не станут ничего исправлять, я публикую свой отчет. Если пытаются затянуть время до полугода - я тоже обнародую данные, почему нет? Если проблема серьезная, нужно устранить ее в отведенное время", - рассказал Чарльза Дардаман.

Многие этичные хакеры говорят, что чувствуют ответственность за информирование пользователей о слабых местах в киберзащите. Когда в компаниях сердятся на то, что хакеры раскрывают потенциальную уязвимость, это говорит о несерьезном отношении фирмы к вопросам безопасности, считает Филипп Уайли. Те, кому сообщают о найденной уязвимости, должны радоваться, что им устроили бесплатный тест на проникновение, убежден ИБ-специалист.