УДК 004.43

Сланова А.В.,
студентка, 3 курс
финансово-экономический факультет
Финансовый университет при Правительстве РФ
Россия, г. Владикавказ
Научный руководитель: Волик М.В.,
кандидат физико-математических наук
Финансовый университет при Правительстве РФ
Россия, г. Владикавказ

БЕЛЫЙ ХАКЕР И ЧЕРНЫЙ ХАКЕР

Аннотация: *Все мы привыкли к тому, что услышав слова «хакер» сразу же представляем себе человека, которого неплохо было бы упрятать в тюрьму, а так же запретить использование всякой электроники на довольно продолжительное время.*

Ключевые слова: *Взлом, информационная безопасность, хакер, интернет, информационные технологии.*

WHITE HACKER AND BLACK HACKER

Annotation: *We all got used to the fact that hearing the words "hacker" immediately imagine a person who would be nice to hide in prison, as well as to prohibit the use of any kind of electronics for quite some time.*

Keywords: *Hacking, information security, hacker, internet, information technology.*

Кто такой черный и кто такой белый хакер?

Чтобы ответить на данный вопрос, нужно определиться со значением этого слова. Хакер, в первоначальном своем значении, указывал на человека, который имел очень хорошие знания в информационных технологиях. В нынешнее же время, хакером все чаще называют тех, кто выявляет слабые места в компьютерных системах, ради забавы или личной выгоды, что всегда представляется окружающим как нечто выходящие за рамки дозволенного. [1, 2] Но у каждого нынешнего хакера свой мотив и поэтому относить всех поголовно к хакерам не стоит. Необходимо их немного разделить.

В основном, под словом «хакер» подразумевают «черных хакеров». Черные хакеры — это те специалисты, которые выявляют слабые места в компьютерных системах и используют их для получения своей выгоды, во вред взломанной компьютерной системе. Но так же бывают и «белые хакеры». Эти, в свою очередь, выявляют уязвимые места в компьютерных системах с целью их устранения. Хотя и они делают это для получения собственной выгоды. Ведь взломанная компьютерная система может заплатить белому хакеру некую сумму в знак признательности и благодарности за оказанную услугу. В любом случае, хакеры, впрочем как и абсолютно большинство населения, надеются получить оплату за свои действия. Белые же хакеры при этом наносят минимальный вред системы, тогда как урон от действий черных хакеров может привести к застою системы.

Кроме озвученных выше хакеров, есть еще и серые хакеры. Серыми хакерами принято называть тех, кто по-немножко тут, и по-немножко там. Такие хакеры при удачном стечении обстоятельств могут слить уязвимость и на черном рынке, хотя при возможности помогают своей репутации стать еще белее, помогая защищать информационные системы.

Кто же из них получает больше за взлом? Черные или белые хакеры? Для ответа на данный вопрос приведу небольшой пример. Некий антивирусный эксперт Джеймс Форшоу получил от Microsoft`а благодарность в размере 100 тысяч долларов за то, что выявил уязвимое место в операционной системе Windows и предоставил возможность Microsoft`у исправить его. И тот же эксперт

получил 9 400 долларов за взлом демо-версии Internet Explorer. А вот Google проводил конкурс с призовым фондом в 1 млн долларов на поиск и выявление уязвимости в Google Chrome (Хотя это не говорит о том, что они готовы были выложить все эти деньги за одну ошибку. Обычно размер призовых зависит от серьезности найденной уязвимости).

Сколько же получают черные хакеры остается только гадать, так как официальную информацию про такие дела никто не озвучивает. Хотя, если у человека на уме нажива, то он вряд ли продаст уязвимость на черном рынке за меньшие деньги. Тем более, что являясь соучастником преступления, нужно заботиться о своей безопасности. А это тоже стоит немалых денег. Поэтому в противостоянии белых против черных выиграют черные хакеры, которых довольно неплохо прячут за решетку.

Поиск уязвимостей напоминает лотерею, в которой можно как сорвать джекпот с кругленькой суммой, так и потерять все, включая свободу. И это вопрос не везения, а четкого понимания границ этичного хакинга. Можно ковырять баги в чужих системах легально.

HackerOne и Bugcrowd. Они, по сути, агрегируют все программы IT-компаний, а зарегистрированные участники сервисов могут выбрать то, что им интересно. Сейчас обе платформы объединяют тысячи специалистов по информационной безопасности из разных стран. Кстати, даже государственные структуры используют подобные сервисы. Например, Пентагон выбрал HackerOne для запуска своей программы Hack the Pentagon.

В конкурсах bug bounty фигурируют очень приличные суммы. В прошлом году компания HackerOne опубликовала отчет Hacker-Powered Security, из которого следует, что в 2017 году среднее вознаграждение за найденный баг составляло более $1 900. Всего за последние 4 года белым хакерам выплатили более $17 млн за 50 тыс. найденных ошибок.

Вообще сказать спасибо за модель bug bounty стоит компании Netscape Communications Corporation. Их сервис Netscape Bugs Bounty, запущенный в середине 90-х, позволял за вознаграждение искать недочеты в браузере Netscape

Navigator. Компания одна из первых догадалась, что лучше своих разработчиков могут быть только тысячи других IT-специалистов, способных за деньги отыскать проблемные места. Идея программы имела такой успех, что ее модель уже очень скоро переняли известные IT-корпорации.

Россия тоже не стоит в стороне. За помощью к белым хакерам обращаются не только крупные компании (Яндекс, Mail.ru, Лаборатория Касперского), но и государство. В этом году в нашей стране запустят централизованную программу по поиску уязвимостей в государственных IT-системах и продуктах вендоров. До конца 2020 года на нее планируется потратить 800 млн рублей. И это очень показательная инициатива: в мире этичный хакинг уже давно стал популярнее и выгоднее криминала: в отличие от несанкционированного взлома, за который светит реальный срок. На bug bounty-программах можно заработать хорошие и, главное, честные деньги.

Когда хакинг может довести до суда

Поиск уязвимостей — это не просто игра, где ты нашел то, что тебе нравится, выбрал оружиеинструмент, нашел баг и выиграл приз. Это целая процедура, у которой есть свой устав. Шаг влево – и «да здравствует наш суд, самый гуманный суд в мире». В чем же дело?

Если у компании нет программы баг баунти - лучше не испытывать судьбу. К примеру, в непростой ситуации оказался 18-летний хакер, которого арестовали за найденную уязвимость на сайте венгерской транспортной компании Budapesti Közlekedési Központ (BKK). С помощью «инструментов для разработчика» в браузере исследователь внес ряд изменений в исходный код страницы и таким образом сумел обмануть систему, «снизив» цену на билеты: с $35 до 20 центов. Юный хакер не стал эксплуатировать уязвимость и по-честному сообщил о баге руководству компании. Но вместо благодарности на него подали заявление в полицию.

Вывод из этого случая прост: участвовать стоит только в официальных конкурсах bug bounty, где все процедуры четко регламентированы. В противном случае – ждите вызова. Принцип «я тихонько взломаю, посмотрю просто из

любопытства, а потом попрошу денег за свою работу» – не прокатит. Для этого даже есть свой термин – Grey Hat.

Любопытно, но конфликты могут быть даже с теми компаниями, у которых есть свои программы баг баунти. Стоит вспомнить случай, когда специалист по безопасности компании Synack Уэсли Вайнберг нашел три уязвимости в инфраструктуре Instagram, благодаря которым он получил доступ практически ко всем конфиденциальным данным приложения. И если за первый баг он получил премию $2,5 тыс., то за второй и третий ему пришлось попотеть. Представители Facebook сообщили исследователю, что он нарушил правила программы Bug Bounty. В официальном заявлении, опубликованном представителями соц.сети, подчеркивалось, что Вайнберг не имел права извлекать пользовательские и системные данные. Его действия были признаны в высшей степени неэтичными. От неприятных последствий со стороны компании его защитило внимание СМИ.

Вывод: быть внимательнее к списку уязвимостей, которые попадают под действие баг баунти, соблюдать политику responsible disclosure и не пытаться получить доступ к личным данным.

УК РФ предупреждает:

Российских хакерам стоит помнить, что УК РФ суров к любым попыткам взлома чужой инфраструктуры. И наказание можно получить сразу по трем статьям (ст. 272, 273, 274), которые грозят не только штрафами, но и реальным сроком за неправомерный доступ к компьютерной информации, распространение вредоносов и нарушение правил хранения, обработки и передачи информации. [3, 4]

Пока в российском законодательстве нет четких определений, какие именно действия по работе с сетевыми ресурсами уголовно наказуемы. Поэтому вопрос границ этичного хакинга очень размыт. И эта неопределенность создает ситуацию, при которой любое сомнительное поведение попадает под внимание спецслужб.

Даже если вашей целью является обучение или тренировка навыков, не стоит необдуманно заниматься активными разведывательными действиями, например: перебирать директории сайтов, использовать прокси (burp) для манипуляции запросов, сканировать порты, использовать сканеры уязвимостей.

Легальный хакинг: без суда и следствия

Теперь поговорим о легальной стороне вопроса. Чтобы получать деньги и славу за bug bounty, необходимо внимательно читать правила конкурса, который запускает компания. Для российских программ могут фигурировать дополнительные требования к участникам, например, «только для граждан России» или «только для налоговых резидентов страны». Важно: сам конкурс должен быть направлен на достижение общественно полезных целей. Если это условие не выполняется, то мероприятие из конкурса превращается в преступную деятельность.

Также в официальной документации программы bug bounty должны быть указаны требования к участникам, сроки проведения и информация о продуктах для тестирования. Организатор должен указать принцип передачи информации о выявленных уязвимостях и порядок ее раскрытия для общего доступа, критерии оценки уязвимостей и, конечно же, информацию о награде. А это самое приятное.

Кто сколько зарабатывает? Российский багхантер Иван Григоров сообщал в интервью, что «по отзывам некоторых топовых хантеров, для них 25 тысяч долларов в месяц — не проблема». Другой пример — багхантер Марк Литчфилд, рассказавший о том, как он за месяц заработал на поиске уязвимостей более $47 000.

Бывают и разовые особенно крупные выплаты. Так в прошлом году Microsoft объявила о запуске программы bug bounty для Windows с максимальной премией в размере $250 000. Деньги обещали за уязвимости в гипервизоре и ядре Microsoft Hyper-V, позволяющие удаленно исполнять код. Немногим ранее Facebook выплатила российскому специалисту по

информационной безопасности Андрею Леонову $40 000 за одну найденную критическую уязвимость.

Google в свое время перечислила экспертам свыше $6 млн, а Facebook за пять лет существования ее «bug bounty» заплатила добропорядочным хакерам $5 млн.

Цифры выше подтверждают, что сейчас bug bounty стал хорошим дополнением к работе или даже основным источником доходов для пентестеров. Чтобы успешно участвовать в таких программах, нужно знать методы поиска и эксплуатации уязвимостей, в первую очередь, в веб-приложениях, а также соблюдать этические нормы и установленные компанией правила.

В любом случае пройти обучение и стать белым хакером гораздо безопаснее и выгоднее, чем идти в криминал. Необходимость в этичных хакерах постоянно растет, а учитывая лавинообразный рост новых IT-областей — блокчейн, big data, IoT — эта потребность будет только увеличиваться.

СПИСОК ЛИТЕРАТУРЫ

1. Козаева К.Г., Плиева В.А., Волик М.В. Информационная безопасность: контроль персонала // Молодежь и наука: актуальные вопросы социально-экономического развития регионов России. Материалы Всероссийской научно-практической конференции, посвященной 95-летию Финансового университета при Правительстве Российской Федерации. 2014. – С. 415-419.

2. Волик М.В. Особенности автоматизации управления предприятием путем внедрения информационных систем // Экономика и предпринимательство. 2017. – № 9-2 (86). – С. 733-736.

3. Волик М.В., Шапранов Н.В. Особенности внедрения информационных технологий на предаприятий // Современные информационно-образовательные технологии в интересах социально-экономического развития России. Международная заочная научно-методическая конференция. 2016. – С. 46-51.

4. Волик М.В., Тедтова И.Э. Зависимость бизнеса от ИТ-инфраструктуры // Современные информационно-образовательные технологии в интересах

социально-экономического развития России. Международная заочная научно-методическая конференция. 2016. – С. 41-45.